TILBURG UNIVERSITY

Tilburg University

Controletechnieken op de werkplaats

de Hert, P.J.A.; Gutwirth, S.

Published in:
Oriëntatie

Publication date:
1993

Document Version
Publisher's PDF, also known as Version of record

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
de Hert, P. J. A., & Gutwirth, S. (1993). Controletechnieken op de werkplaats: Herbeschouwing in het licht van het persoonsgegevensbeschermingsrecht deel 2. *Oriëntatie*, *5*, 125-147.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 05. May. 2023

Controletechnieken op de werkplaats :

herbeschouwing in het licht van «persoonsgegevensbeschermingsrecht» (deel 2)

Paul DE HERT en Serge GUTWIRTH,
Interdisciplinary Research Unit on Information Security
Centrum voor Internationaal Strafrecht
Vrije Universiteit Brussel

In het eerste deel van deze bijdrage (gepubliceerd in het vorige nummer van *Oriëntatie*) werd een overzicht gegeven van de feitelijke en juridische stand van zaken rond controletechnieken op de werkplaats, in het bijzonder wanneer zij onaangekondigd of geheim worden ingezet. In voorliggend tweede deel wordt de materie opnieuw opgenomen, maar vanuit een meer prospectieve hoek.

Daarbij wordt ingegaan op de Franse situatie, waar via een ruime Wet op de verwerking van persoonsgegevens een soepel juridisch beschermingssysteem werd uitgewerkt dat (tevens) van toepassing is op controletechnieken (II). O.i. beschikt België al langer dan vandaag over de juridische mogelijkheden om dezelfde weg op te gaan, meer bepaald op basis van een samenlezing van artikel 8 van het E.V.R.M. en een aantal internationale teksten die de basisbeginselen van het recht m.b.t. de verwerking van persoonsgegevens hebben vastgelegd (I). Met de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (verder : de Privacywet) (1) rijst thans de vraag hoe die wet – die duidelijk geïnspireerd is door zijn Franse tegenhanger – in België toegepast zal moeten worden, teneinde ook hier te komen tot de uitbouw van een soepel juridisch beschermingssysteem dat (tevens) van toepassing is op controletechnieken (III en IV).

I. De basisprincipes inzake gegevensbescherming

1. Enkele opmerkelijke vonnissen

De Luikse Rechtbank van Eerste Aanleg (2) besliste in 1987 dat «de fundamentele mensenrechten en in het bijzonder het recht op bescherming van de privacy» werden aangetast door de oprichting en terbeschikkingstelling van een databank van geheime zwarte lijsten van slechte debiteurs «zonder enige rekening te houden met de verdere ontwikkeling van het krediet en zonder verwijdering na verloop van tijd of na afbetaling van de lening of na een gerechtelijke beschikking die vaststelt dat de schuldvordering niet bestaat of dat geen fout in hoofde van de schuldenaar kan weerhouden worden». Opmerkelijk is dat de rechter – zonder verwijzing naar enige preciese rechtsbron, buiten de aanhaling van het E.V.R.M. – er door toepassing van de aquiliaanse aansprakelijkheid, toch toe komt preciese criteria voorop te stellen waaraan het houden van een databank moet beantwoorden (3). Zo achtte hij in het bijzonder het recht op inzage en verbetering essentieel. Op 5 juni 1991 werd deze uitspraak in beroep bevestigd op basis van een parallel lopende redenering (4).

In een soortgelijke zaak veroordeelde de vrederechter te Namen een kredietverzekeraar die aan een bank foutieve gegevens had verstrekt over de eiser, die daardoor een kredietaanvraag geweigerd zag (5). Te dezen haalde de rechter zowel artikel 8 van het E.V.R.M. aan, als het (niet door België geratificeerde) Verdrag tot bescherming van personen ten opzichte

van de geautomatiseerde verwerking van persoonsgegevens en het toen actueel zijnde Belgische wetsontwerp «voor databanken» (6). Uit deze regels «die van kracht zijn of nog van kracht moeten worden» distilleerde de vrederechter gedragsnormen die door alle houders van registraties moeten nageleefd worden : de gegevens moeten juist en bijgewerkt zijn en de betrokkene heeft een inzage- en verbeteringsrecht. Deze regels werden *in casu* niet nageleefd.

De genoemde uitspraken illustreren duidelijk dat het E.V.R.M. directe werking heeft in de interne rechtsorde en dat zijn *self-executive* bepalingen door de burgers kunnen ingeroepen worden voor de nationale rechter (7). Het Verdrag behoort trouwens tot de «Europese openbare orde», wat inhoudt dat het ambtshalve door de rechter moet opgeworpen worden, alsook dat het de voorkeur verdient boven ermee strijdige interne wetgeving (8). Daaruit voortvloeiend heeft uiteraard ook artikel 8 van het E.V.R.M. (9) directe werking in het Belgische recht en primeert het op ermee strijdige wetgeving (10).

Tevens geven de aangehaalde beslissingen gestalte aan de thans gevestigde stelling dat het E.V.R.M. en de grondrechten die het erkent – de fundamentele waarden van de Westerse beschaving – functioneren in *alle* maatschappelijke interacties, d.w.z. zowel in «verticale» publiekrechtelijke als in «horizontale» privaatrechtelijke verhoudingen (11).
Dat geldt in het bijzonder voor de privacy (12).

Dit alles impliceert dat elke handeling die door een rechtssubject als privacykrenkend wordt ervaren, de artikel 8 van het E.V.R.M.-toets moet ondergaan en dit los van de vraag of de handelende persoon een overheidsorgaan of een burger is. Maar hoe ziet die toets er uit ?

Wat de verticale verhouding Staat-burger betreft, is de zaak vrij duidelijk (13). Artikel 8 van het E.V.R.M. voorziet dat de in het eerste lid gewaarborgde vrijheid van het privéleven onder bepaalde voorwaarden door de Staat beperkt of aangetast kan worden. Die voorwaarden zijn, zoals ze door het Hof te Straatsburg worden geïnterpreteerd, vierledig. In de eerste plaats moet de aantasting bij wet voorzien worden (formeel criterium) (14). Ten tweede kan zij uitsluitend geschieden voor zover zij nodig is in een democratische samenleving (noodzakelijkheidscriterium) én zulks, ten derde, alleen ter verwezenlijking van bepaalde, limitatief in alinea 2 opgesomde wettige doeleinden (legitimiteitscriterium). Ten vierde moet nagegaan worden of het vooropgestelde doel niet had kunnen bereikt worden door een maatregel die de gewaarborgde vrijheid in mindere mate zou aangetast hebben (proportionaliteitscriterium (15)).

Zonder scherpe scheidslijnen te trekken tussen de verschillende criteria wegen het Hof te Straatsburg en de nationale rechters in het gestelde kader de belangen van Staat en burger aan elkaar af, daarbij rekening houdend met hun respectieve inworteling in de normenhiërarchie (16).

Meer onzekerheid heerst er rond de vraag onder welke voorwaarden burgers – b.v. werkgevers – de privacy kunnen krenken in de rechtsorde van het E.V.R.M. Ter zake spreekt Van der Heijden over «onbestemd proza» (17). Die onbestemdheid heeft natuurlijk te maken met de tekst van artikel 8, alinea 2 van het E.V.R.M., die enkel bakens legt voor de beoordeling van de schending van de privacy door de overheid (*cf. supra*). Via de rechtspraak zou deze onduidelijkheid weggenomen kunnen worden.

Er moet echter vastgesteld worden dat artikel 8 van het E.V.R.M. desbetreffend weinig gebruikt wordt. De vaststelling geldt vooral voor arbeidsrechtelijke geschillen. Van der Heijden merkt m.b.t. Nederland op dat de arbeidsrechtspraak de horizontale werking heeft geconcretiseerd aan de hand van specifiek op de arbeidsverhouding toegesneden begrippen. We treffen afwegingen aan tussen de plichten van «goede werknemers» en «goede werkgevers», vaak resulterend in de vraag of er al dan niet sprake is van «dringende redenen» om tot ontslag over te gaan (18).

Omtrent artikel 8 is er bijgevolg maar schaarse sociaalrechtelijke rechtspraak en dat bemoeilijkt elk synthesewerk van de rechtsleer. Als voorbeeld kunnen we verwijzen naar de KOMA-camera-zaak, die besproken werd in het eerste deel van deze bijdrage. Het is het énig voorhanden zijnde arrest over cameracontrole, en daarin speelden concrete feiten (nl. de stand van de camera's) een zodanig grote rol, dat de vaagheid omtrent principes wel moet blijven bestaan.

Dezelfde vaagheid treft ook België, waar rechtspraak die gebruik maakt van artikel 8 van het E.V.R.M. eveneens schaars is. Recentelijk veroordeelde de Arbeidsrechtbank van Brussel het gebruik van verborgen videocamera's op basis van strijdigheid met artikel 16 van de Wet op de arbeidsovereenkomsten, waardoor sprake is van een gebrek aan eerbied en achting van de werkgever t.a.v. de werknemers (19). Wat Van der Heijden opmerkt voor Nederland geldt

ook hier : de rechtbank lost een privacygeschil op met behulp van een typisch arbeidsrechtelijk instrumentarium (20).

De diversiteit van problemen opgeworpen door controletechnieken, het gegeven dat er daarover nauwelijks cassatierechtspraak is (*cf.* deel 1), de verscheidenheid van de lagere rechtspraak (*id.*) ontnemen ook hier de doctrine een stevige steun om gefundeerde richtlijnen te geven over controletechnieken in het licht van de mensenrechten en het E.V.R.M. Rauws en Schyvens geven m.b.t. de privacy enkel richtsnoeren inzake sollicitatie- en ontslagproblemen. Hun vaststelling «dat ook het grondrecht van privé-leven van de werknemer aan beperkte beperkingen onderhevig is» wordt niet verder uitgewerkt (21).
Humblet, die zowel Belgische als Nederlandse rechtspraak citeert die respectievelijk verborgen en aangekondigde cameracontrole op werknemers veroordeelt, vindt dat dergelijke controles niet altijd afgewezen mogen worden. Rechters moeten z.i. belangen afwegen en het belang van de werkgever kan in sommige gevallen het gebruik van T.V.-circuits rechtvaardigen. Hij haalt daarbij een hypothese aan die betrekking heeft op de beveiliging van fietsenstallingen (22). Hierbij moet aangestipt worden dat dergelijke richtlijnen van auteurs een louter argumentatieve waarde toekomt. Het laatste woord is aan de rechter, die zich op de wet steunt.
Dat dit in het kader van artikel 8 van het E.V.R.M. *niet* tot een patstelling leidt, bewijzen de reeds besproken uitspraken van de Luikse en Naamse rechters.

Tweemaal lag immers een conflict te berde waarover specifieke Belgische wetgeving ontbrak, wat hen ertoe bracht terug te vallen op de door België erkende supranationale normen «die van kracht zijn of nog van kracht moeten worden». Het braakland, door artikel 8 van het E.V.R.M. gevormd, wordt alzo in kaart gebracht aan de hand van basisprincipes van gegevensbescherming die de juridische contouren van de privacy verder uitwerken. Het is onze overtuiging dat deze supranationale normen een onbenut potentieel vormen. In het kader van de Raad van Europa werden teksten uitgevaardigd waarin de *data protection*-normen specifiek op controletechnieken worden toegepast.
Het loont de moeite om er even bij stil te staan.

2. De supranationale normen

In grote lijnen treft men de basisprincipes inzake de automatische verwerking van persoonsgegevens aan in de O.E.S.O.-Richtlijnen (23) en het Verdrag van Straatsburg (24).

Ze zijn eveneens aanwezig in het door de Commissie van de Europese Gemeenschappen ingediend C.E.G.-gewijzigd voorstel van privacyrichtlijn (25). De inhoud van deze teksten is telkens zeer gelijklopend.

2.1. De O.E.S.O.-Richtlijnen

De niet-bindende O.E.S.O.-Richtlijnen van 23 september 1980, die door de 24 O.E.S.O.-lidstaten werden onderschreven, veruiterlijken een consensus over een aantal fundamentele principes die de basis vormen van de thans bestaande privacywetten : ze functioneren als een *general framework* of startpunt voor de elaboratie van wetgeving ter zake (26). De O.E.S.O.-Richtlijnen beogen de bescherming van alle persoonsgegevens, te weten gegevens over *natuurlijke* personen, ongeacht de wijze (automatisch of manueel) waarop zij verwerkt worden.

Afwijkingen van de principes kunnen slechts geschieden om redenen van nationale veiligheid, soevereiniteit en openbare orde : zij moeten uitzonderlijk zijn en publiek gemaakt worden (art. 1 tot 6 O.E.S.O.-Richtlijnen).

De zgn. «basisprincipes inzake bescherming van persoonsgegevens» (art. 7 tot 14 O.E.S.O.-Richtlijnen) zijn (27) :
1. het *collection limitation principle*, krachtens hetwelk de opslag van bepaalde (niet nader door de richtlijnen omschreven) gevoelige gegevens beperkt moet worden; elke verzameling van persoonsgegevens moet tevens wettelijk en eerlijk geschieden met toestemming of wetenschap van de betrokkene;
2. het data quality principle, krachtens hetwelk de gegevens relevant behoren te zijn voor het doel waarvoor ze verwerkt worden en tevens – in het licht van dit doel – volledig, accuraat en *up to date* dienen te zijn;
3. het *purpose specification principle*, krachtens hetwelk de persoonsgegevens in het licht van een omschreven en gespecificeerd doel moeten worden verzameld;
4. het *use limitation principle*, krachtens hetwelk de gegevens niet voor een ander doel dan het omschreven doel mogen gebruikt worden behoudens toestemming van de betrokkene of een verplichtende wettelijke bepaling;
5. het *security safeguards principle*, krachtens hetwelk de gegevens technisch beschermd moeten worden tegen verlies, beschadiging, ongeoorloofde toegang;
6. het *openess principle*, krachtens hetwelk eenieder op de hoogte moet kunnen zijn van bestaande hem betreffende gegevensbestanden, hun

doel en gebruik en het adres van hun verantwoordelijke beheerder;
7. het *individual participation principle*, krachtens hetwelk het individu het recht heeft om de gegevens hem betreffende te localiseren, op te vragen, na te gaan en de verbetering ervan te eisen;
8. het *accountability principle*, krachtens hetwelk voor elk bestand een beheerder wordt aangeduid die verantwoordelijk is voor de naleving van de principes.

2.2. Het Verdrag van Straatsburg

Dit in de schoot van de Raad van Europa onderhandelde verdrag, dat op 1 oktober 1985 in werking trad, sluit aan bij artikel 8 van het E.V.R.M. Het verdrag heeft tot doel het recht op persoonlijke levenssfeer van elke natuurlijke persoon die zich op het grondgebied van een toetredende Staat bevindt, te waarborgen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (art. 1).

Het verdrag betracht *in globo* – zoals de O.E.S.O.-Richtlijnen – een harde kern van maatregelen voor de bescherming van de persoonlijke levenssfeer tegenover de geautomatiseerde verwerking van persoonsgegevens in het nationale recht van de toetredende partijen in te voeren.

Zijn bepalingen zijn bindend, maar niet *self-executing* (28) : de door het verdrag toegekende rechten kunnen er niet rechtstreeks aan ontleend worden. Elke verdragspartij moet in haar intern recht de noodzakelijke maatregelen treffen teneinde de in het verdrag vervatte principes te bekrachtigen (art. 4). België ondertekende het verdrag op 7 mei 1982, maar het heeft tot 8 december 1992 geduurd alvorens een nationale rechtsnorm – de Privacywet – daaraan zou kunnen tegemoet komen (29).

Het verdrag is van toepassing op automatisch verwerkte persoonsgegevens betreffende natuurlijke personen, zowel in de private als in de openbare sector. Niettemin wordt aan de toetredende staten de mogelijkheid geboden om de werkingssfeer uit te breiden tot manueel verwerkte gegevens en gegevens over rechtspersonen. Ook wordt in een procedure voorzien waarbij zij kunnen beslissen dat bepaalde categorieën van gegevens niet onder de toepassing van het verdrag zullen vallen (art. 3) (30). Artikel 4 *et seq.* van het verdrag bevatten de «grondbeginselen van gegevensbescherming». Deze verschillen nauwelijks van de O.E.S.O.-beginselen. Noch het verdrag, noch de O.E.S.O.-Richtlijnen verlenen aan de persoon het recht om zich te *verzetten* tegen de automatische opslag of verwerking van gegevens hem betreffende.

De Raad van Europa heeft zich niet beperkt tot het aanbevelen van de (grote) basisbeginselen inzake *gegevensverwerking*. Het ministercomité van de Raad heeft op basis van de werkzaamheden van het *Committee of experts on data protection* (niet-bindende, maar wel gezaghebbende) specifieke aanbevelingen gericht tot de lidstaten.

Zulke sectoriële aanbevelingen werden reeds gegeven op het vlak van medische gegevensbestanden (R(81)1), databanken voor statistisch en wetenschappelijk onderzoek (R(83)10), gegevens gebruikt voor *direct marketing* (R(85)20), databanken van de sociale zekerheid (R(86)1), politionele databanken (R(87)15), gegevens voor betalingen of verwante verrichtingen (R(90)19) en gegevens gebruikt met betrekking tot tewerkstelling (R(89)2).

Dit laatste document bevat richtlijnen m.b.t. de bescherming van persoonsgegevens wanneer deze aangewend worden voor werkgelegenheidsdoeleinden (31). Uit R(89)2 citeren we volgende passages («aanbevelingen») :
– aanbeveling 2 m.b.t. de eerbiediging van de persoonlijke levenssfeer en de menselijke waardigheid van werknemers luidt : «Respect for the privacy and human dignity, in particular the possibility of exercising social and individual relations at the place of work, of the employee should be safeguarded in the collection and use of personal data for employment purposes»;
– aanbeveling 3, lid 1 en 2 m.b.t. de kennisgeving en consultatie van werknemers luidt : «In accordance with domestic law or practice and, where appropriate, in accordance with relevant collective agreements, employers should, in advance, fully inform or consult their employees or the representatives of the latter about the introduction or adaptation of automated systems for the collection and use of personal data of employees. This principle also applies to the introduction or adaptation of technical devices designed to monitor the movements of productivity of employees (3.1.). The agreement of employees or their representatives should be sought before the introduction or adaptation of such systems or devices where the consultation procedure referred to in paragraph 3.1. reveals a possibility of infringement of employees' right to respect for privacy and human dignity unless domestic law or practice provides other appropriate safeguards (3.2.)»;
– aanbeveling 4, lid 4 m.b.t. het verzamelen van gegevens luidt : «Re-

course to tests, analyses and similar procedures designed to assess the character or personality of the individual should not take place without his consent or unless domestic law provides other appropriate safeguards. If he so wishes, he should be informed of the results of these tests»;
– aanbeveling 6, lid 2 m.b.t. het (intern) gebruik van persoonsgegevens luidt : «Where data are to be used for employment purposes other than the one for which they were originally collected, adequate measures should be taken to avoid misinterpretation of the data in the different context and to ensure that they are not used in a manner incompatible with the original purpose. Where important decisions affecting the employee are to be taken, based on data so used, he should be informed».

3. Het belang van de basisprincipes

De werkzaamheden van de O.E.S.O. en de Raad van Europa vormen een beleidsgerichte reflectie over informaticaproblemen, zelfs al betreffen sommige initiatieven ook manuele bestanden. Het bestaan van de informatica heeft evenwel geen nieuw privacyprobleem geschapen, maar wel een aantal zaken scherper gesteld. Het is onze overtuiging dat de in internationale verdragen geformuleerde basisprincipes een zeer breed toepassingsdomein bestrijken, dat verder gaat dan het nogal enge domein van de verwerking van persoonsgegevens op *geautomatiseerde wijze*. Dat moge duidelijk blijken uit de zopas geciteerde aanbeveling R(89)2. In het verlengde liggend van artikel 8 van het E.V.R.M. moeten de *data protection principles* beschouwd worden als dragers van een door de Westerse maatschappij beoogd niveau van privacybescherming, dat normstellend is in het kader van alle mogelijke vormen van verwerking van persoonlijke informatie, ongeacht of er al dan niet computers meespelen.

De gevolgtrekking ligt voor de hand : resulteert een bepaalde – manuele, geautomatiseerde, visuele ... – handeling in het verzamelen van gevoelige informatie, dan moet de rechter naar de basisbeginselen inzake gegevensverwerking grijpen teneinde eventuele lacunes in de rechtsbescherming tegen dergelijke handelingen te dichten. Bovendien vindt de gevolgtrekking steun in de vaststelling dat vele door rechtspraak en rechtsleer geformuleerde oplossingen, moeiteloos vertaald kunnen worden in de termen van de basisbeginselen.

De spontaan door Blanpain (32) geformuleerde richtlijnen m.b.t. aids en drugs komen er op relevante wijze mee overeen, niettegenstaande die gegroeid zijn uit «diepgaande gesprekken met collega's juristen, geneesheren en bedrijfsleiders» en niet uit één of andere theoretische deductie.

Wanneer de Nationale Arbeidsraad m.b.t. de privacyproblematiek bij de werving en selectie bepaalt dat «vragen over het privé-leven slechts verantwoord zijn indien zij relevant zijn voor de functie» (art. 11 C.A.O. nr. 38), dan treffen we hier een toepassing aan van het relevantieprincipe (*data quality principle*) en het finaliteitsbeginsel (*purpose* specification principle).

De toepassing van de beginselen inzake gegevensbescherming heeft trouwens al resultaten opgeleverd. Personeelsprofielen opgesteld zonder medeweten van de werknemer zijn oncontroleerbaar. In Nederland heeft men via de wetgeving op de verwerking van persoonsgegevens in hoofde van de werknemers een inzagerecht in die profielen erkend, waardoor de bestaande wettelijke lacune gedeeltelijk (33) gedicht werd (*individual participation principle*). De Europese richtlijn inzake het werken met beeldapparatuur bepaalt dat bij gebruik van software door werknemers er zonder hun medeweten geen gebruik mag worden gemaakt van een kwantitatief of kwalitatief controlemechanisme (34). We zien hier een toepassing van het transparantie- of open-vizierprincipe (*openess principle*), krachtens hetwelk eenieder op de hoogte moet kunnen zijn van de bestaande hem betreffende gegevensbestanden, hun doel, hun gebruik en het adres van hun verantwoordelijke beheerder.

Het belang van het transparantieprincipe mag niet onderschat worden : een correcte toepassing verzet zich immers tegen elke geheime aanwending van spionage- en controletechnieken op het bedrijf. De reeds geciteerde aanbeveling 3.1. uit R(89)2 is wat dat betreft zeer duidelijk (*cf. supra*). Het is m.a.w. ontoelaatbaar om zonder enige raadpleging spionagetechnieken in te voeren. In de inleiding van het eerste deel van deze bijdrage verhaalden we hoe de délégés van een autoconstructiebedrijf instemden met de door de werkgever in het geheim uitgevoerde drugtests, die pas later aan het licht kwamen. Op deze wijze verzaakten de délégés o.i. aan een fundamenteel recht inzake privacy, nl. dat de titularis van het recht op de hoogte moet gebracht worden van elke voorgenomen krenking van zijn privacy. Niet alleen maakte de handelwijze van de patroon het de individuele werknemer of sollicitant onmogelijk om de test te weigeren, maar ook kregen de werknemers via hun collectieve vertegenwoordiging niet het forum om over de

tests onderhandelingen te openen. Uit dit voorbeeld blijkt o.i. waarom het transparantiebeginsel cruciaal is. Eerbiediging ervan maakt het mogelijk dat over privacy onderhandeld of tenminste gesproken kan worden.

Het *openess principle* strookt wat controletechnieken betreft bovendien met de basisfilosofie van de Wet op de arbeidsreglementen. Krachtens deze wet moet er melding gemaakt worden van alle manieren aangewend door de werkgever om de arbeid te controleren (35).

Dezelfde filosofie treffen we ook aan in C.A.O. nr. 39 m.b.t. de invoering van nieuwe technologieën, die stelt dat een informatie- en consultatieprocedure moet opgestart worden telkens wanneer een nieuwe technologie met «belangrijke sociale consequenties» geïntroduceerd wordt in de werkplaats (36). Ontegensprekelijk heeft de invoering van een personeelsvolgsysteem een «belangrijke sociale consequentie». In het gebruik van een prikklok of enig ander middel moet door het reglement voorzien worden, evenals in de wijze waarop er gebruik van wordt gemaakt. Zolang de werkgever geen afschrift (van een wijziging) van het arbeidsreglement aan zijn werknemer overhandigd heeft, is de werknemer niet gebonden door de bepalingen van dit reglement. Niets staat o.i. een toepassing van het transparantieprincipe in de weg, wanneer in een geschil verborgen technieken aan de orde worden gesteld. Het ontbreken van wetgeving maakt de rechter niet machteloos.

Poullet en Warrant zijn in navolging van de Luikse en Naamse rechters op zoek gegaan naar oplossingen voor controlemiddelen in de bestaande internationale verdragen m.b.t. gegevensverwerking. Hun werkwijze bestaat in wat ze noemen een «relecture» van het Verdrag van Straatsburg (37). Met behulp van de hierin vervatte *data protection-guidelines*, werkten ze een systeem uit waarbij zowel de belangen van de werkgever als de rechten van de werknemer verzoend worden, o.a. bij de telefooncontrole en -registratie. Hun aanpak verdient navolging. De materie van de controletechnieken kan zelden met korte verbodsbepalingen gevat worden. We illustreren dat aan de hand van het voorbeeld waarbij camera's ingezet worden ter beveiliging van fietsenstallingen. Voor Humblet lijkt het verdedigbaar dat camera's worden geïnstalleerd omdat «de werkgever, bewaarnemer, in geval van fietsendiefstal moet kunnen bewijzen dat hij aan zijn bewaringsverplichting de nodige zorg heeft besteed» (38).

Een evaluatie van dezelfde situatie in het licht van de basisbeginselen van gegevensbescherming biedt o.i. meer garanties. Dat leidt immers tot volgende overwegingen. De installatie moet in elk geval openlijk, eerlijk en rechtmatig gebeuren (*openess en collection limitation*) en na toestemming van de werknemers of hun vertegenwoordigers (aanbeveling 3 R(89)2), in het kader van een welomschreven doelstelling (finaliteitsbeginsel) en dat wel voor zover de installatie van de camera's nuttig en onontbeerlijk is t.a.v. de fietsenbeveiliging, én ze geen disproportionele inmenging betekent in de privacy van de werknemers vergeleken met het nagestreefde doel (*proportionaliteit*) (39). Bovendien mogen de verzamelde beelden niet langer bijgehouden worden dan noodzakelijk is voor het doel en kunnen ze niet voor enig ander doel aangewend worden (*use limitation*)... Al bij al lijkt het hier gewoon beter om vaststaande sloten ter beschikking te stellen of om in een gesloten ruimte te voorzien – waarmee géén privacykrenking gepaard gaat – tenzij de praktijk dan nog uitwijst dat fietsen verdwijnen.

Besluiten we hierover dat de rechter, geconfronteerd met conflicten m.b.t. personeelsvolgsystemen, in de internationale teksten rond gegevensbescherming voldoende aanknopingspunten vindt om – bij ontstentenis van wetgeving – oplossingen uit te werken die tegemoetkomen aan een ernstige privacybescherming van de werknemer.

Onverminderd de reeds vastgestelde mogelijkheden van de rechter (art. 8 E.V.R.M., *data protection principles*) wordt in het volgende deel van onze bijdrage nagegaan of een «relecture» van de Privacywet kan leiden tot hetzelfde resultaat. Dat zal geschieden in wisselwerking met de lectuur van het C.E.G.-gewijzigd voorstel van privacyrichtlijn, doch niet voordat eerst wordt ingegaan op het Franse recht, dat op voorbeeldige wijze de brug heeft gelegd tussen *data protection* en arbeidsrecht.

II. De Franse Privacywet : de creatieve interpretatie door de C.N.I.L.

1. Inleiding

De Franse rechtspraak heeft steeds het gebruik van spionagemiddelen afgewezen : op geheime wijze verzameld bewijsmateriaal is frauduleus en mag ter zitting niet aangewend worden, zoniet ontstaat er «un espionnage continuel», «un intolérable

climat de méfiance» tussen werkgever en werknemer (40). De werkgever moet de aan te wenden methodes niet alleen aankondigen (openheid), hij moet in de eerste plaats alleen die controlemethodes kiezen die afgestemd zijn op de te controleren situatie (finaliteit) en daarbij een redelijk evenwicht respecteren tussen zijn belang en de privacy van de werknemer(s) (proportionaliteit) (41). De genoemde rechtspraak vond daarbij steun in de krachtlijnen door de wetgever uitgezet in drie wetten.

Het meest recent zijn de Wetten Auroux m.b.t. «les nouveaux droits des travailleurs» (1982). Deze bepalen o.m. dat de ondernemingsraad geraadpleegd moet worden over elk plan tot introductie van nieuwe technologieën indien ze een weerslag hebben op de arbeidsvoorwaarden van het personeel. Een echt controlerecht voor de ondernemingsraad op de verzamelde gegevens wordt evenwel niet georganiseerd (42).

Ook het Strafwetboek vormt een aanknopingspunt. Tegen het onderscheppen door derden van elektronische boodschappen wordt artikel 187 van de C.P. ingeroepen, dat aan de post toevertrouwde boodschappen beschermt (43). Dit is evenwel een moeilijke strafbepaling omdat kwaad opzet vereist is. Zo werd een nieuwsgierige werkgever vrijgesproken omdat de gesloten enveloppe, geadresseerd aan een werknemer, niet alleen diens naam vermeldde, maar ook deze van het bedrijf (44). In 1970 werd artikel 368 van de C.P. ingevoerd dat het heimelijk opnemen of filmen in een private plaats bestraft (45). Ook de werkplaats valt hieronder. Binnen het bedrijf is het bijgevolg verboden in het geheim gesprekken van werknemers af te luisteren, op welk ogenblik ook tijdens de uitvoering van hun arbeidscontract. Dit verbod geldt zowel voor niet voor het publiek toegankelijke bedrijfslokalen (de kantine) als voor bedrijfslokalen waarin werknemers vertoeven en het publiek slechts op bepaalde tijdstippen toegang heeft (46). Ook het werken met videocamera's valt onder het toepassingsdomein van het verbod (47). Een bepaalde rechtspraak acht artikel 368 van de C.P. niet van toepassing op het capteren van louter professionele gesprekken. Het Parijse Hof van Beroep heeft aan die polemiek een (voorlopig) eind gemaakt : het volstaat dat een gesprek wordt afgeluisterd, er moet niet nagegaan worden of het betrekking had op privacygevoelige topics (48).

Artikel 368 van de C.P. is niet van toepassing op het registreren van gesprekken en beschermt ook niet de bedrijfslokalen die wel voor het publiek toegankelijk zijn.

Voor deze juridische hiaten heeft men een oplossing gezocht in de «Loi nr. 78-17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés» (49). Deze wet, die aan de O.E.S.O-Richtlijnen en het Verdrag van Straatsburg vooraf ging, draagt in zich de kiemen van de internationale basisprincipes inzake gegevensbescherming en richt een autonome privacycommissie op, nl. de Commission nationale de l'informatique et des libertés (C.N.I.L). De C.N.I.L. waakt over de toepassing van de in de wet neergelegde rechten, verschaft informatie, kan bemiddelen bij klachten, ziet toe op de naleving van de wet, kan waarschuwingen richten en overtredingen van de wet aangeven bij het parket. Bovendien bezit ze reglementaire bevoegdheid (b.v. het uitvaardigen van «normes simplifiés» voor de aangifte van verwerkingen).

2. Het arbeidsrecht en de Franse Privacywet

De Wet van 6 januari 1978 is zeer ruim geformuleerd en werd al snel toegepast op arbeidsrechtelijke problemen. Via een subcommissie (informatique et liberté du travail) worden hoorzittingen over arbeidsrechtelijke privacyvraagstukken georganiseerd. Met de resultaten stelt de C.N.I.L. aanbevelingen (50) en «normes simplifiés» op. Het resultaat is indrukwekkend.

– Voor de C.N.I.L. valt elk individueel personeelsdossier onder het toepassingsdomein van de wet, wanneer dit het uitvloeisel vormt van een al dan niet geautomatiseerde «fichier» (51). Een werkgever die bij derden verzamelde syndicale en politieke gegevens optekent in manuele bestanden, miskent de Wet van 6 januari 1978.
Wel verenigbaar is het uithangen binnen het bedrijf van een bulletin dat aangeeft hoeveel tijd syndicale vertegenwoordigers gebruiken voor hun syndicale plichten (52).
In het algemeen wordt het inwinnen van informatie die niets te maken heeft met het beroep – b.v. bij sollicitatie – door de C.N.I.L. afgeraden (53).

– Artikel 2 van de Wet van 6 januari 1978 verbiedt elke besluitvorming gebaseerd op profielen opgesteld aan de hand van via automatische systemen verzamelde gegevens. Een ontslag op loutere basis van prikklokgegevens kan bijgevolg niet aanvaard worden. Hetzelfde geldt voor geautomatiseerde sollicitatiepakketten. In een aanbeveling heeft de C.N.I.L. de consequenties van de Wet van 6 januari 1978 (inzagerecht, mededelingsplicht, ...) uitdrukkelijk neergeschreven met het oog op een regle-

mentering van de sollicitatie-adviesbureaus (54). N.a.v. klachten over sollicitatiepakketten die naast objectieve en professionele ook psychologische criteria hanteren waarvan de sollicitant niet op de hoogte is, heeft de C.N.I.L. opnieuw een soortgelijke aanbeveling gedaan.
M.b.t. deze automatische persoonlijkheidstesten wordt gevraagd dat ze aanvangen met een vermelding van de rechten neergelegd in de Franse Privacywet. Beslissingen moeten rekening houden met de professionele ervaring van de kandidaat en met de uitslag van een gesprek. De test alleen volstaat bijgevolg niet. Bovendien moet elke geteste persoon toegang kunnen krijgen tot de uitslag, alsmede tot de interpretatie die hieraan gekoppeld wordt (55).
Van geautomatiseerde sollicitatietesten stappen de C.N.I.L. en de Franse rechtspraak over op sollicitatietesten *tout court*. Dat blijkt uit volgende zaak : een werkgever liet een door een sollicitant geschreven tekst zonder diens medeweten onderwerpen aan een handschriftstudie (meten van psychologische capaciteiten). Met succes werd hiertegen de Wet van 6 januari 1978 ingeroepen, die gegevensgaring verbiedt «opérée par tout moyen frauduleux, déloyal ou illicite» (56).
De C.N.I.L. heeft, geconfronteerd met aangiften van grafologische softwareprogramma's, gewezen op haar onbevoegdheid om over de betrouwbaarheid ervan uitspraak te doen, maar zij heeft van het bedrijf dat ze commercialiseert, bekomen dat bij elke verkoop in het contract melding zou gemaakt worden van het engagement van de cliënt de Privacywet te respecteren (57).

– Ook op elektronische identificatiebadges werd de Privacywet toegepast (58).
Het vergaren van gegevens via elektronische badges verschilt immers niet wezenlijk van de gewone automatische gegevensverwerking. De door de C.N.I.L. ontwikkelde beginselen verplichten de werkgever duidelijk te maken welk gebruik van de badges wordt gemaakt.
Slechts in uitzonderlijke gevallen en voor een beperkte periode kunnen gegevens via het badgegebruik verzameld worden. De werkgever moet binnen het bedrijf afzien van identificatieprocedures, wanneer die niet strikt noodzakelijk zijn. Dat geldt volgens de *Garde des sceaux* ook voor de vermelding van de naam en voornaam van de betrokkenen op de werkkledij (59).

– Reeds in 1982 bepaalde de C.N.I.L. dat France Télécom aan de telefooneigenaars slechts gedetailleerde facturen mocht verstrekken mits weglating van de laatste vier cijfers van de opgeroepen nummers (60). Controle van de factuur is aldus mogelijk zonder dat precies uitgemaakt kan worden welke nummers opgeroepen werden, waardoor rekening gehouden wordt met het telefoongeheim van zij die het toestel gebruiken.
Telefoonregistratieapparaten werden vanaf 1984 door de C.N.I.L. aan volgende voorwaarden onderworpen : voorafgaande consultatie van de werknemers, informatie over de uitoefening van controle via affichage en kleine snelberichten, behoud van de gegevens alleen toegelaten voor de facturatie, bescherming van bepaalde lokalen (o.a. die van de délégés) en verbod op belemmering van de uitoefening van de rechten van beschermde werknemers (61).
Het onaangekondigd controleren van telefoongesprekken door werkgevers is bijgevolg onder het toepassingsdomein van de Wet van 6 januari 1978 gebracht, wat recentelijk leidde tot een eerste veroordeling van een Franse werkgever (62).
Bekendmaking van het telefoongebruik van bepaalde werknemers aan derden (o.a. aan de valva's lijsten hangen van de langste «telefoneerders») is verboden krachtens artikel 29 van de Wet van 6 januari 1978, dat de gegevensverzamelaar verbiedt deze door te geven «à des tiers non autorisés» (63). Opgemerkt weze nog dat facturen ogenschijnlijk niet onder het toepassingsgebied van de wet vallen, maar omdat het opvragen van telefoonfacturen eenzelfde doel beoogt als de telefoonregistratieapparaten zou controle via facturen zonder voorafgaande waarschuwing van de werknemers neerkomen op een oneerlijk middel in de zin van artikel 25 van de Franse Privacywet, aldus de C.N.I.L. (64).

– Het Franse Hof van Cassatie heeft in 1991 het gebruik van verborgen camera's veroordeeld. Wat nu met niet-verborgen cameracontrole ?
Via de Wet van 6 januari 1978 verklaarde de C.N.I.L. zich bevoegd t.a.v. klachten over het gebruik van digitale camera's oordelend dat «l'image constitue également une information ... au sens de la loi du 6 janvier 1978 dès lors que l'individu représenté peut être identifié» (65).
Camera's zijn onderworpen aan de basisprincipes inzake gegevensverwerking (voorafgaande mededelingsplicht, proportionaliteitsbeperking...).
De C.N.I.L. heeft recentelijk het licht op groen gezet voor twee video-surveillance-experimenten (in de Parijse ondergrondse en rond een commercieel complex) telkens onder voorwaarden : geen camera's op deuringangen, verwittiging van het publiek, regels m.b.t. inzage en stockage van de beelden (66).

III. De Belgische Privacywet : een te interpreteren wet

1. Algemeen

De Belgische Privacywet werd uiteindelijk op 18 maart 1993 in het *Staatsblad* gepubliceerd. Dat betekent dat België er na meer dan 15 jaar voorstellen, ontwerpen en «epileptische» regeringen eindelijk (67) in is geslaagd een Privacywet te maken, die voldoet aan de algemene principes van gegevensbescherming (68).

In globo streeft de Privacywet naar een evenwicht «tussen de vereisten van de bescherming van de persoonlijke levenssfeer en de vereisten van het bestuurlijk, economisch en sociaal bestel» (69).

Artikel 2 stelt als principe dat eenieder bij de verwerking van persoonsgegevens die op hem betrekking hebben, het recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Over dit recht beschikte de natuurlijke persoon evenwel al krachtens artikel 8 van het E.V.R.M. Het recht neergelegd in artikel 2 is bovendien beperkt tot de eerbiediging van de privacy «bij de verwerking van persoonsgegevens». Het toepassingsgebied bestrijkt *manuele en automatische* bestanden van persoonsgegevens (over natuurlijke personen) in de *private en openbare sector*.

Tevens bevat de wet de krachtlijnen inzake gegevensverwerking van persoonsgegevens, alsmede de uitzonderingen op deze krachtlijnen (o.a. gegevens voor politioneel gebruik) (70).

Tenslotte is een lange reeks strafrechtelijke bepalingen opgenomen (art. 37 tot 43) die betrekking hebben op zowat alle verplichtingen die uit de wet voortvloeien. Er wordt in hoge boeten voorzien naar analogie met deze in financiële, economische en milieuwetgevingen, teneinde inbreuken op de beschermde fundamentele vrijheid door rechtspersonen effectief te bestrijden (71).

Van belang is verder dat de Privacywet de werking en bevoegdheden van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer op definitieve wijze bepaalt en organiseert (art. 23 tot 36) (72).

De genoemde commissie is thans titularis van een «algemene controlebevoegdheid over alle bestanden en gegevensverwerkingen» (73). D.w.z. dat ze op elk ogenblik de gegevens uit de aangifte kan raadplegen, gegevens kan opeisen (art. 17 § 4), een onderzoek kan instellen tot het bekomen van meer informatie (art. 32), gemotiveerde aanbevelingen kan richten (art. 30)...

Tevens behoort de commissie in een reeks door de wet voorziene gevallen door de regering voor advies geraadpleegd te worden.

De commissie verkrijgt tenslotte een degelijke zelfstandige onderzoeksbevoegdheid, kan zich laten bijstaan door deskundigen (art. 32 § 1), en heeft bemiddelingsbevoegdheden met betrekking tot klachten, onverminderd enig rechtsmiddel voor de rechtbanken (art. 31).
Zij behoort, tenzij de wet anders bepaalt, bij het parket aangifte te doen van vastgestelde misdrijven (art. 32 § 2). Haar voorzitter moet ieder geschil m.b.t. de wet en haar uitvoeringsbesluiten aan de rechtbank van eerste aanleg voorleggen (art. 32 § 3).

2. Arbeidsrechtelijke gevolgen van de Privacywet

De onmiddellijke gevolgen van de nieuwe wet zijn aanzienlijk : de werkgever mag niet (meer) om het even wat opslaan, verwerken en combineren voor om het even welke doeleinden. De wet is immers ook van toepassing op de manuele of automatische verwerking van persoonsgegevens in de onderneming. Een overzicht van de in de wet vervatte plichten.

De openbaarheid van *geautomatiseerde* verwerkingen van persoonsgegevens wordt bewerkstelligd door een voorafgaande aangifteplicht bij de commissie, die er een openbaar register van bijhoudt («het bestandenbestand»). Een hele reeks gegevens moeten verstrekt en in het register opgenomen worden (o.a. de identiteit van de houder van het bestand, de oorsprong van de gegevens, de categorieën verwerkte gegevens, het doel van de verwerking, ...). Met betrekking tot manuele bestanden kan de commissie, wanneer zij meent dat er gevaar dreigt voor de persoonlijke levenssfeer, dezelfde inlichtingen inwinnen.

Op advies of voordracht van de commissie kan de Koning geautomatiseerde verwerkingen van persoonsgegevens die kennelijk geen gevaar inhouden voor de persoonlijke levenssfeer, van aangifte vrijstellen of toestaan dat een aangifte met een beperkt aantal vermeldingen zou worden gedaan. Dat is het systeem van «vereenvoudigde aangiften» (74).

De verwerking van bepaalde gevoelige gegevens (o.a. de syndicale of mutualistische affiliatie) wordt in beginsel verboden, of precieser uitgedrukt : zij is slechts toegelaten voor

door of krachtens de wet vastgestelde doeleinden. Medische en gerechtelijke gegevens worden evenzeer onderworpen aan een bijzonder regime, waarin hun verwerking door de werkgever een schriftelijke toestemming van de betrokkene vergt (art. 7).

Het finaliteitsbeginsel – dat de hoeksteen is van de wet – heeft tot gevolg dat de gegevensverwerking (registratie, bewaring, wijziging, de uitwissing, raadpleging of verspreiding) enkel mag geschieden in functie van vooraf bepaalde doeleinden, die bovendien wettig en duidelijk omschreven moeten zijn (art. 5). Een koppeling tussen personeelsgegevens en individuele gegevens, gemeten tijdens het produktie- of dienstverleningsproces, kan niet zomaar doorgevoerd worden (75). Het afstaan van een personeelsbestand om het te gebruiken in sociale verkiezingen is ook niet toegelaten (76). Rechtspersonen met verschillende activiteiten, zoals een bank die zich ook met verzekeringen inlaat of een distributiemaatschappij die aan *direct mailing* participeert, zullen de onderscheiden gegevensverwerkingen van elkaar moeten afsluiten en scheiden (77) (78).

Ook het *collection-limitation principle* werd neergelegd in artikel 5 van de Privacywet : uitgaande van het doel van de verwerking moeten de gekozen gegevens toereikend, terzake dienend en niet-overmatig zijn. De aard van de gegevens moet overeenkomen met het beoogde doel van de verwerking. Dat kan beoordeeld worden aan de hand van de proportionaliteitsregel (79).
Globaliserend impliceert de formulering van artikel 5 van de Privacywet dat voldaan moet worden aan een viertal voorwaarden : 1, de gekozen doelstelling van de verwerking moet afgebakend zijn (vereiste van de finaliteitsafbakening); 2, zij moet tevens duidelijk omschreven en wettig zijn (formele en materiële wettigheidvereiste); 3, de gekozen gegevens moeten voor dat doel toereikend, ter zake dienend en niet-overmatig zijn (conformiteitsvereiste) en 4, zij mogen niet gebruikt worden op een wijze die met het doel onverenigbaar is (vereiste van het verenigbaar gebruik). Over de naleving van het finaliteitsbeginsel zal door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer gewaakt worden. In voorkomend geval zullen geschillen dienaangaande kunnen voorgelegd worden aan de rechtbanken. Elke schending van artikel 5 is strafbaar met een correctionele straf (art. 39).

Elke betrokkene heeft een recht op inzage en op kosteloze verbetering van gegevens die hem betreffen (art. 10 en 12). Ook kan de verwijdering of het verbod van aanwending geëist worden van gegevens die, gelet op het doel van de verwerking, onvolledig of niet ter zake dienend zijn, of nog van gegevens waarvan de verwerking verboden is of die te lang werden bijgehouden. De voorzitter van de rechtbank van eerste aanleg neemt kennis van dienaangaande vorderingen (art. 14). Ook hier is strafvervolging mogelijk.

Problematisch in de wet is wel de uitwerking van het open-vizierprincipe : bij de eerste verzameling van persoonsgegevens bij de betrokkene moet deze ingelicht worden over alle gegevens die hij nodig zal hebben voor de uitoefening van zijn recht op inzage en verbetering (art. 4). Indien de gegevens bij derden worden ingewonnen, moet de betrokkene onverwijld op de hoogte gesteld worden van de eerste registratie waarvan hij het voorwerp vormt, *tenzij* de verwerking kadert in een contractuele of wettelijke relatie tussen houder van het bestand en betrokkene (80).

Deze regeling is voor kritiek vatbaar. Een werknemer wiens gegevens worden opgenomen in het bedrijfsinformatiesysteem, is alleen op de hoogte als de gegevens «bij hem verzameld worden» (art. 4) en niet als de gegevens via derden of uit andere bestanden worden verzameld teneinde verwerkt te worden in het kader van een contractuele relatie (81). Wat loont een recht op inzage en correctie, indien de open-vizierplicht wordt uitgehold binnen contractuele relaties door toe te laten dat het bestaan van sommige verwerkingen niet wordt bericht aan de betrokken werknemers ? Juist naar aanleiding van contractuele relaties (inzonderheid arbeids- en bediendenovereenkomsten) worden veel bestanden aangelegd... (82).

Dit gaat regelrecht in tegen de O.E.S.O.-Richtlijnen en de aanbeveling (R(89)2) van de Raad van Europa m.b.t. de bescherming van persoonsgegevens aangewend voor werkgelegenheidsdoeleinden. Deze laatste bepaalt immers dat persoonsgegevens in principe alleen bij het personeelslid zelf mogen worden ingewonnen. Wanneer men gegevens buiten de contractuele verhouding wil betrekken, moet de betrokkene minstens worden ingelicht (aanbeveling R(89)2, 4.1.).

Bij sollicitanten, moet de informatie bij henzelf ingezameld worden, en is de toestemming vereist vooraleer gegevens aan derden mogen gevraagd worden (aanbeveling R(89)2, 4.1.). De doorgave van de ingezamelde gegevens aan derden kan slechts geschieden hetzij krachtens een wettelijke verplichting, hetzij na kennisgeving (wanneer de communicatie

strookt met het doel van de originele inzameling), hetzij na uitdrukkelijke en geïnformeerde toestemming van de betrokkene (aanbeveling R(89)2, 8.1. en 8.2.).

Steunend op artikel 2 van de Belgische wet dat aan ieder een recht op eerbiediging van zijn persoonlijke levenssfeer erkent bij de verwerking van persoonsgegevens, zal men moeten waken over het dat er via een ruime interpretatie van artikel 9 geen uitholling van de rechten van de geregistreerde werknemer plaatsvindt (83).

Het C.E.G.-gewijzigd voorstel van privacyrichtlijn is over deze kwestie gelukkig duidelijker (*cf. infra*). Overigens zal de rechter de bedoelde disproportionele praktijken steeds kunnen beoordelen in het licht van de directe werking van artikel 8 van het E.V.R.M., geïnterpreteerd aan de hand van de *data protection principles* (*cf. supra*).

In tegenstelling tot artikel 28 van de Nederlandse Wet persoonsregistraties (84), dat uitdrukkelijk voorziet in een schriftelijke mededeling, binnen de maand na de eerste registratie, zegt de Belgische Privacywet niets over de vorm van de kennisgeving (85) en weinig over het tijdstip ervan. De Privacywet voorziet overigens niet in een voorafgaande melding, maar dat strookt met de logica van de wet, daar het Belgisch systeem, in tegenstelling tot het Franse, geen blokkeringsrecht toekent aan de betrokkenen (86). De initiatiefnemende minister stelde evenwel dat artikel 9 moet uitgelegd worden in die zin dat kennisgeving onmiddellijk moet geschieden, tegelijk met de aanvang van de verwerking (87). Het gevaar blijft echter bestaan dat men een loopje gaat nemen met die «onverwijlde» kennisgeving. Teneinde het verrassingseffect van bepaalde verwerkingen van persoonsgegevens te counteren, zal de commissie hierop nauwgezet moeten toekijken.

3. Vallen personeelsvolgsystemen onder de toepassing van de Privacywet ?

De wet zegt niets specifieks over spionagetechnieken of personeelsvolgsystemen. De voorbereidende werkzaamheden maken evenwel her en der allusie op de problematiek. Zo benadrukken de Memorie van Toelichting en de initiatiefnemende minister dikwijls dat de wet zich uitsluitend beperkt tot één aspect van de bescherming van de persoonlijke levenssfeer, met name de verwerking van persoonsgegevens. Expliciet wordt daarbij verwezen naar de problematiek van het afluisteren van telefoongesprekken en het bespieden. Hierover laat de regering duidelijk verstaan dat ze in de toekomst van plan is reglementerend op te treden (88). Dat is hoe dan ook nog niet gebeurd. Niettegenstaande de duidelijke stellingnamen van de minister is de problematiek van de controletechnieken tijdens het totstandkomingsproces van de wet aan de orde gesteld door sommige leden van de Privacycommissie, tijdens hun *hearing* in de senaatscommissie. Op de vraag van een senator of de wet ook van toepassing moet geacht worden op camera's en audiovisuele technische apparatuur wanneer personen gefilmd worden (89), mocht blijken dat de leden van de commissie het daarover niet eens zijn. Een commissielid stelde dat in de huidige stand van zaken beeldbanden niet vallen onder de wet, maar hij voegde daaraan wel onmiddellijk toe dat de technieken naar elkaar toegroeien en dat de digitalisering van beeld- en klankmateriaal zeer denkbaar is, zodat «de tijd niet meer veraf is dat dat materiaal binnen het toepassingsgebied van de wet zal vallen» (90). Daarentegen was een ander lid van mening dat de definities van de wet zich niet verzetten tegen de interpretatie van beeld- en klankgegevens als persoonsgegevens (91).

Het is aan de hand van de in artikel 1 opgenomen definities dat moet onderzocht worden in welke mate de wet toepasbaar is op personeelsvolgsystemen (audiovisuele en elektronische monitoring; profielen) (92).

Eerste vaststelling : de wet doelt op persoonsgegevens, zijnde gegevens die betrekking hebben op een natuurlijke persoon die is of kan worden geïdentificeerd (art. 1 § 5). Gegevens die informatie belichamen (93) kunnen bestaan uit tekens (taal), maar ook uit geuren, beelden en geluiden. Foto's, beelden, opnamen, films, sensoren, ... bevatten gegevens. Kunnen die gegevens iets zeggen over een bepaalde persoon, dan zijn het persoonsgegevens (94).

Tweede vaststelling : opdat de wet toepasselijk zou zijn, moeten deze persoonsgegevens het onderwerp zijn van een verwerking d.w.z. hetzij van een geautomatiseerde verwerking, hetzij van een gehouden manueel bestand. Daarbij wordt het «houden van een manueel bestand» gedefinieerd als de registratie, de bewaring, de wijziging, de uitwissing, de raadpleging of de verspreiding van persoonsgegevens in de vorm van een bestand op een niet-geautomatiseerde drager (art. 1 § 4), met dien verstande dat «bestand» wordt begrepen als een geheel van persoonsgegevens die op een logisch gestructureerde wijze zijn samengesteld en bewaard met het oog op een systematische raadpleging ervan (art. 1 § 2) (95). Onder «geauto-

matiseerde verwerking» wordt daarentegen verstaan : «elk geheel van bewerkingen die geheel of gedeeltelijk langs geautomatiseerde weg zijn uitgevoerd en betrekking hebben op de registratie en de bewaring van persoonsgegevens, alsook op de wijziging, de uitwissing, de raadpleging of de verspreiding van deze gegevens» (art. 1 § 3).

Uit deze definities volgt dat België, in tegenstelling tot sommige buurlanden, de voorwaarde van het «bestand» alleen heeft gehandhaafd wat manuele gegevens betreft. Dat is logisch, want zodra persoonsgegevens, zelfs zonder enige logische structuur, op geautomatiseerde wijze geregistreerd zijn, kunnen zij met behulp van eenvoudige programmatuur op een systematische manier worden geraadpleegd.

Indien de Privacywet de vereiste van een bestand voor alle verwerkingen had behouden, dan zouden ten onrechte talrijke geautomatiseerde verwerkingen buiten schot gevallen zijn. In het huidig stelsel stelt de werkgever die de elektronische postbus van zijn werknemers doorsnuffelt, een handeling die valt onder het toepassingsdomein van de wet (96). Daarentegen valt, zoals gezien, het cryptisch omschreven *houden van een manueel bestand* enkel en alleen onder de Privacywet wanneer er sprake is van een ordening van de gegevens.

Dit laat toe om ook niet-geautomatiseerde verwerkingen onder de wet te brengen, maar toch ergens een grens te trekken in de zee van persoonsgegevens die voorkomen op niet-geautomatiseerde dragers.

Dumortier en Claes stellen de vraag of videobanden en geluidscassettes niet-geautomatiseerde dan wel geautomatiseerde dragers zijn (97). Wij geloven dat het laatste het geval is : deze banden en cassettes vormen immers het eindpunt van een procédé waarbij automatisering komt kijken. Blijkt uit de toepassing van de wet dat het gaat om niet-geautomatiseerde dragers, dan «houdt» de werkgever die gebruik maakt van audiovisuele spionage- en controletechnieken – zodra hij de tapes voor raadpleging systematiseert – wel degelijk «een manueel bestand» en is hij onderworpen aan de in de wet opgesomde plichten van «houders van manuele bestanden» (*cf. infra*).

Geluidsregistraties, foto's en videoopnamen verschaffen informatie die toelaat natuurlijke personen te identificeren. Wil dat nu zeggen dat het opnemen, fotograferen of filmen *geautomatiseerde verwerkingen* kunnen genoemd worden volgens artikel 1, § 3 van de Privacywet ? Dat zal alleszins zo zijn inzake camerabewaking, wanneer de films worden bewaard. Immers, de verwerking is «geautomatiseerd» omdat het voldoende is dat in een keten van bewerkingen er één voorkomt die geautomatiseerd verloopt (het trekken van een foto) (98). Aan de bijkomende eis dat de geautomatiseerde verwerking betrekking moet hebben «op de registratie en de bewaring van persoonsgegevens, alsook op de wijziging, de uitwissing, de raadpleging of de verspreiding van deze gegevens», komt de camerabewaking met bewaring van films zeker tegemoet (99). En dat betreft een groot deel van de gevallen.

Vraag : hoe zit het nu met bewaking zonder bewaring ? De tekst van artikel 1, § 3 is verwarrend tengevolge van gebruik van de voegwoorden «en-of». Moet er sprake zijn van een registratie *en* een bewaring, of volstaat een registratie ? Men zou kunnen stellen dat, gegeven de definitie van het houden van een manueel bestand (waarin enkel «of» wordt gebruikt), het niet gaat om cumulatieve voorwaarden : het registreren «of» bewaren volstaat. Zoniet zou camera- of telefoonbewaking waarvan de resultaten op band worden gezet, wel onder het begrip «geautomatiseerde verwerking» vallen, maar dezelfde handelingen zonder bewaring niet, niettegenstaande zij op dezelfde wijze haaks staan op artikel 8 van het E.V.R.M. De werkgever die de elektronische post van zijn werknemers op het scherm oproept, doch deze niet bewaart, zou dan ontsnappen aan het toepassingsdomein van de wet, terwijl degene die deze gegevens zou laten uitdraaien of op diskette vastlegt, wél onder de wet zou vallen...

Daarentegen brengt de gelijkschakeling van de loutere raadpleging met een automatische verwerking onwerkbare consequenties mee : elke automatische verwerking moet dan aangegeven worden. Het is raadzaam dat de commissie deze kwestie verduidelijkt, vooral wat zulke spionagetechnieken betreft die beslist een inmenging betekenen in de persoonlijke levenssfeer.

4. Aangifteplicht

Zowel de houders van geautomatiseerde verwerkingen als die van manuele bestanden moeten beiden een aantal voorwaarden van de wet respecteren (o.a. respect van het finaliteitsbeginsel, verbod op verwerking gevoelige gegevens, verlenen van toegangs- en correctierecht).

Het grote verschil zit in de openbaarheidsplicht, d.w.z. de voorafgaande aangifteplicht van artikel 17, die in principe slechts de eerste categorie betrokkenen treft.

Op die aangifte, die voor elke geautomatiseerde verwerking geldt, moet naast het doel van de verwerking ook de wijze vermeld staan waarop de personen op wie de gegevens betrekking hebben, daarvan in kennis worden gesteld, de dienst waarbij het recht op toegang kan worden uitgeoefend en de maatregelen genomen om de uitoefening van dat recht te vergemakkelijken. De commissie legt een register aan van dergelijke aangiften, dat ter inzage ligt van eenieder. Op elk stuk waarvoor de verwerking wordt gebruikt, moet het identificatienummer van de verwerking vermeld staan waardoor eenieder in het register informatie kan bekomen over het wie, hoe en waarom van de automatische verwerking. De commissie kan deze aangifteplicht ook opleggen voor bepaalde manuele bestanden, als zij meent dat ze een mogelijke schending van de persoonlijke levenssfeer inhouden (art. 19).

Het openbaar register is in zijn praktische organisatie nog niet rond, maar vormt het logisch sluitstuk van een rechtsbeschermingssysteem dat ondanks de mogelijkheden van de nieuwe techniek aan de burger toch nog enige controle wil verschaffen over het gebruik van gegevens m.b.t. zijn persoon. In de hierboven aangenomen veronderstelling dat controletechnieken een «geautomatiseerde verwerking» vormen, betekent een consequente toepassing van de wet dat de aanwending van zo'n technieken altijd (dus ook wanneer ze «geheim» zijn) via de omweg van het publiek register toch kenbaar moet zijn aan eenieder. Blijkt dat een surveillancesysteem niet is aangegeven, eventueel omdat men het in het geheim wil laten werken, dan is de houder strafbaar.
De aangifteplicht voor geautomatiseerde verwerkingen en voor manuele bestanden, in de hypothese voorzien in artikel 19, heeft tot gevolg dat *elke* (100) controletechniek uiteindelijk aan het licht zou moeten komen.

5. Rechtmatige geheime methodes ?

Rijst verder de vraag of geheime controle überhaupt verenigbaar is met de globale principes van de Privacywet ? Het algemeen geformuleerde basisbeginsel van artikel 5 van de Privacywet bevat geen vergelijkbare bewoordingen als die van artikel 25 van de Franse Privacywet, waarin elke gegevensgaring expliciet verboden wordt wanneer die bedrieglijk, oneerlijk of onrechtmatig is («frauduleux, déloyal ou illicite»). Deze bepaling sluit aan bij het eerlijkheidsbeginsel (*collection limitation principle*) dat krachtens artikel 5 van het Verdrag van Straatsburg als volgt wordt geformuleerd : «Persoonsgegevens die langs automatische weg verwerkt worden dienen (...) op *eerlijke* en wettige wijze te worden verkregen en verwerkt».

De Raad van State en de Commissie voor de Bescherming van de Persoonlijke Levenssfeer drongen erop aan dat ook bij ons het eerlijkheidsbeginsel expliciet in de wet zou opgenomen worden (101). Dat deze raad uiteindelijk niet werd opgevolgd, betekent nochtans niet dat het eerlijkheidsbeginsel niet van kracht is. Zo stelde een lid van de commissie tijdens de *hearings* dat het beginsel wél in aanmerking zal genomen worden, daar de commissie zich bij het beoordelen van de verwerking zal moeten laten leiden door het Verdrag van Straatsburg (102). Tevens zal de commissie steeds, en in het bijzonder na elke aangifte, moeten nagaan of de verwerkte persoonsgegevens «op ongeoorloofde manier zijn ingezameld, zonder iemand te informeren» (103). Dat de gegevens op eerlijke wijze moeten verkregen worden, betekent opnieuw – zeker in het kader van een wet die de openheid en kennisgeving van de inzameling huldigt – dat geheime of verborgen methodes resoluut als onrechtmatig dienen beschouwd te worden (*cf.* C.N.I.L.).

Rest de vraag of de commissie bevoegd is inzake personeelvolgsystemen. Wij denken van wel. De commissie heeft daar trouwens in haar adviezen i.v.m. het wetsontwerp zelf, zij het dan op onrechtstreekse wijze, voor gepleit. Dat gebeurde doorheen haar voorstel om aan artikel 2 van de wet een algemenere draagwijdte te geven, door de toevoeging van de tekst : «De verwerking dient de rechten van de mens en de fundamentele vrijheden te eerbiedigen» (104). Op deze manier pleitte ze, met verwijzing naar de Franse situatie, voor de uitbreiding van de werking van de waarborgen geboden door de wet naar alle door de Grondwet en het E.V.R.M. beschermde rechten en vrijheden. Krachtens deze formulering zou zij immers een ruimer actieterrein verkrijgen, dat zeker het veld van de controletechnieken omvat. Deze aanpassing is o.i. niet noodzakelijk om de bevoegdheid van de commissie ter zake te staven, want de bedoelde systemen zijn wel degelijk «verwerkingen» van persoonsgegevens die een gevaar betekenen voor de persoonlijke levenssfeer.

Het voorgaande impliceert *a fortiori* dat de rechter personeelssystemen kan beoordelen in het licht van de Privacywet. Anders dan de commissie echter, zal de rechter dat *alleszins* mogen doen op basis van een samenlezing van artikel 8 van het E.V.R.M. en de basisbeginselen van gegevensbescherming (*cf.* de Luikse en Naam-

se rechters). Dat betekent dat hij zich ter zake zelfs niet zal moeten buigen over de vraag of de bedoelde personeelssystemen «verwerkingen» zijn in de zin van de Privacywet. Alleen de bevoegdheid van de commissie hangt daarvan af, niet de zijne. De rechter zal o.i. in de genoemde samenlezing alle juridische elementen kunnen vinden om verborgen of zelfs onaangekondigde spionagetechnieken onrechtmatig te verklaren.

6. Arbeidsrechtelijke beoordeling

Delarue merkt reeds op dat verschillende basisbeginselen, gehanteerd in het persoonsgegevensbeschermingsrecht, stroken met vigerende arbeidsrechtelijke regels (105). Het verbod te werken met gegevens over ras en politieke overtuiging is reeds opgenomen in I.A.O.-Conventie 111 (106). Artikel 22 van de Wet van 12 april 1965 op de loonbescherming legt een inzage- en transparantierecht op t.v.v. de werknemer die zo toezicht kan uitoefenen «op alle verrichtingen dienend om de hoeveelheid of de hoedanigheid van de verrichte arbeid vast te stellen en alzo het bedrag van het loon te bepalen». In C.A.O. nr. 39 (inzake de invoering van nieuwe technologieën) (107) en C.A.O. nr. 9 (inzake personeelsbeleid en organisatie van het werk) (108) treffen we eveneens een meldings- en consultatieplicht aan. Ook Dumortier en Claes wijzen op deze wetgeving om lacunes in de Privacywet m.b.t. de meldingsplicht te dichten.

Van de geciteerde rechtsbronnen wordt evenwel, naar ons weten, nooit gebruik gemaakt voor de rechter wat problemen aangaande controletechnieken betreft. Bovendien wordt de C.A.O. nr. 39 door de werkgevers niet spontaan nageleefd (109).

O.i. is de Privacywet, zoals reeds gestaafd, een noodzakelijke aanvulling op het bestaande arbeidsrechtelijke instrumentarium (*cf.* de cameracontrole op fietsenstallingen). Maar de toepassing van de wet op de surveillance, het doorzoeken van de elektronische post en de profielen is geen sinecure. De wet getuigt van een gebrek aan (technisch) vooruitzicht van de wetgever die zich al te zeer toegespitst heeft op de economische noden van de gegevensverwerking in hun conflict met individuele burgers, wat een aandachtsgebrek t.a.v. collectieve arbeidsverhoudingen verklaart.

Vergelijkt men de Belgische (1992), Nederlandse (1989) en de Franse Privacywet (1978) dan stellen we het volgende vast : de werkplaats is vergeten, terwijl ze in vele opzichten het natuurlijk strijdtoneel vormt van de gegevensverwerking (110). Wat op de werkplek op het spel staat, is niet zozeer de intimiteit, maar eerder het recht van werknemers zich te beschermen tegen beslissingen die van invloed zijn op hun levensomstandigheden en op hun fundamentele zelfbeschikkingsvrijheid. De werkplek is een plaats waar bij uitstek dergelijke beslissingen genomen worden.

De Franse wet van 1978 (de oudste van de drie) is evenwel van meet af aan ruim opgevat en besteedt o.a. aandacht aan profielen, aan de inzameling van gegevens en voorziet het recht op verzet. Dat laat toe om de gegevensbescherming beter op werkverhoudingen af te stemmen. Daarbij beschikt de C.N.I.L. over voldoende speelruimte om zulks waar te maken. In Frankrijk zijn de *data protection principles* meer dan alleen van toepassing op gegevensbestanden : ze vormen de neerslag van een (maatschappelijke) positiebepaling over privacy in het algemeen.

De Belgische wet kopieert voor één keer het Franse voorbeeld te weinig. Het is te hopen dat met behulp van de «minor problems» die wel geregeld zijn, door de activiteiten van de nog jonge privacycommissie, en door een volgehouden creatieve inspanning van de rechtspraak en rechtsleer, een brug geslagen wordt tussen het leven binnen en het leven buiten de werkplaats. Een belangrijke – en dwingende – impuls daartoe zou wel eens uit Europese hoek kunnen komen.

IV. Het initiatief van de Europese Gemeenschappen : duidelijke taal

1. Voorgeschiedenis

De niet-ondertekening of niet-ratificatie van het Verdrag van Straatsburg door sommige Lid-Staten (België, Portugal, ...), houdt in de ogen van de E.G.-Commissie een gevaar in voor het handelsverkeer binnen de interne markt.
Zo zouden Lid-Staten die het verdrag geratificeerd hebben, gegevensuitwisseling met andere Lid-Staten kunnen reglementeren of verbieden, onder het voorwendsel dat er in laatstgenoemde landen onvoldoende bescherming wordt verzekerd. Het vrij verkeer van persoonsgegevens vereist dat overal een gelijkwaardig, hoog (111) beschermingsniveau van persoonsgegevens wordt gehaald. Ter realisatie van dat oogmerk maakte de Commissie van de Europese Gemeenschappen een eerste voorstel van privacyrichtlijn bekend (112).

Tegen de voorgestelde richtlijn kwam evenwel reactie vanuit de bedrijfs- en bankwereld : het voorstel werd te streng en onevenwichtig bevonden, te

bureaucratisch, te gericht op verzameling en aanwezigheid van gegevens, te stroef, onhoudbaar, een catastrofe voor de economie, enz. (113). Maar ook de vergadering van *EC Data protection commissioners* verzette zich o.a. tegen de zwakke bevoegdheden van de in de richtlijn georganiseerde «Groep voor de bescherming van persoonsgegevens» en de verzwakking van het vereiste criterium voor de doorgave van persoonsgegevens naar derde landen (114).

Het voorstel werd dus aangevallen wegens een *te veel* én een *te weinig*. Het Europees Parlement nam in de twee jaar die ondertussen verstreken zijn, ongeveer honderd wijzigingsvoorstellen aan. Niet zo lang geleden heeft de Commissie het gewijzigd Voorstel van Privacyrichtlijn bekendgemaakt. Het is de bedoeling dat de richtlijn *medio* 1993 wordt vastgesteld.

2. Inhoud van het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn

De voorgestelde privacyrichtlijn heeft betrekking op de «behandeling» van geautomatiseerde en manuele gegevens. Een onderscheid wordt gemaakt al naargelang de behandeling geautomatiseerd is of niet : voor manuele behandelingen moet het gaan om een bestand, voor geautomatiseerde behandelingen niet (*cf.* België) (115).

Persoonsgegevens hebben betrekking op een geïdentificeerde of identificeerbare persoon (*cf.* Verdrag van Straatsburg). Het begrip «persoonsgegeven» is van toepassing «op alle informatie die op een natuurlijk persoon betrekking kan hebben (...). Een persoon kan ofwel direct geïdentificeerd worden aan de hand van een naam ofwel indirect aan de hand van een telefoonnummer, een autokenteken, een SoFi- of soortgelijk nummer, een paspoort (...) De definitie heeft eveneens betrekking op gegevens als beelden en stem, vingerafdrukken en erfelijke eigenschappen» (116). De uitbreiding naar visuele en auditieve gegevens is dus expliciet (117).

Ook «behandelen» wordt ruim gedefinieerd (118) : de term slaat op alle verrichtingen «van het verzamelen tot en met het verwijderen en de daartussenliggende handelingen» (119). Het louter verzamelen van gegevens is bijgevolg een behandeling (120), wat ook blijkt uit artikel 3.1 dat de werkingssfeer van de richtlijn, wat betreft niet-geautomatiseerde behandelingen, uitbreidt tot persoonsgegevens die «bestemd zijn om daarin te worden opgenomen». De uit de richtlijn voortvloeiende beginselen van bescherming zijn niet afhankelijk «van bepaalde technologie of technische organisatie; het begrip behandeling van gegevens biedt de mogelijkheid tot het ontwikkelen van een algemene aanpak waarbij de aandacht is gericht op de gebruikte gegevens en op het geheel van activiteiten waarop die gegevens betrekking hebben met het oog op de nagestreefde doelstellingen» (121). Dat betekent dat automatische visuele controle, alsook het elektronisch corresponderen (E-mail) (122) onder de voorgenomen richtlijn zullen vallen.

In artikel 6 vinden we een aantal basisbeginselen van het Verdrag van Straatsburg terug, hier ook toepasselijk op niet-geautomatiseerde gegevensbestanden (*collection limitation, data quality, purpose specification en use limitation*). Persoonsgegevens kunnen slechts behandeld worden indien deze behandeling «eerlijk en rechtmatig» is (art. 6 lid 1 a). Dit sluit het gebruik uit van verborgen apparatuur waarmee buiten weten van de betrokkenen gegevens verkregen worden. Deze bepaling verbiedt eveneens clandestiene behandelingen uit te voeren of te gebruiken (123).

In het voorstel wordt niet uitdrukkelijk gewag gemaakt van een mededelingsplicht aan geregistreerden bij opname van dier gegevens in een behandeling, maar deze eis vloeit voort uit artikel 7 van het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn dat de voorwaarden stelt waaronder gegevensbehandeling toegelaten is. De behandeling van persoonsgegevens is slechts rechtmatig, wanneer «de betrokkene zijn toestemming daarvoor heeft verleend» (art. 7a). Zonder toestemming is ze tevens rechtmatig, wanneer ze noodzakelijk is in het kader van een contractuele relatie met de geregistreerde of voor de uitvoering van precontractuele maatregelen waarmee op een verzoek van de betrokkene wordt ingegaan (art. 7b), wanneer er sprake is van een verplichting die door de Europese of nationale wetgever is opgelegd (art. 7c), wanneer de behandeling noodzakelijk is teneinde de primaire belangen van betreffende geregistreerde te beschermen (art. 7d), wanneer de behandeling noodzakelijk is ten behoeve van taken in het openbaar belang of in het kader van publiekrechtelijke taken van de houder of derden, aan wie de persoonsgegevens zijn verstrekt (art. 7e) en wanneer de behandeling noodzakelijk is voor het algemeen belang of voor de rechtmatige belangen van de houder, of van derden, aan wie de gegevens zijn verstrekt, behalve in die gevallen, waarin de belangen van de geregistreerde prevaleren (art. 7f) (124).

Het is artikel 7b dat werkgevers toelaat gegevens over werknemers te ge-

bruiken in het kader van de uitvoering van contractuele afspraken. Behelst de behandeling méér dan b.v. de betalingen van de salarissen, dan moet er sprake zijn van toestemming. De werkgever krijgt zo weinig beslissingsruimte, aldus Berkvens en Schauss die bovendien geloven dat in geval van een conflict het belang van de werknemer zal prevaleren (*cf.* art. 7f) (125).

Onze analyses wijzen nochtans een andere richting uit : de privacybescherming van werknemers blijkt dikwijls zeer fragiel t.a.v. het economische belang.

Onder toestemming (waarvan sprake in art. 7a) verstaat het voorstel elke uitdrukkelijke wilsuiting waarmee de betrokkene aanvaardt dat persoonsgegevens worden behandeld, mits de betrokkene over inlichtingen beschikt omtrent het doel van de behandeling, omtrent de gegevens of categorieën van gegevens waar het bij de behandeling om gaat, omtrent de personen voor wie de persoonsgegevens zijn bestemd en omtrent de naam en het adres van de voor de behandeling verantwoordelijke. De toestemming is specifiek en mag door de betrokkene te allen tijde zonder terugwerkende kracht worden ingetrokken (art. 2g). De toestemming kan zowel schriftelijk als mondeling zijn, maar ze moet in ieder geval vrij zijn, vooral «in die situaties waarin mogelijkerwijs druk kan uitgeoefend worden op de betrokkene (b.v. in de situatie werknemer/werkgever)» (126).

Elke behandeling van persoonsgegevens moet worden aangemeld aan de nationale toezichthoudende autoriteit (art. 18) (127), wat de betrokkene toelaat de in artikel 13 neergelegde rechten op rectificatie, verwijdering en afscherming uit te oefenen.

3. Rechten van de betrokkenen

In hoofdstuk II en III van het voorstel worden de rechten van de betrokkenen uitgewerkt : deze heeft het recht om op verzoek in kennis gesteld te worden van het feit dat er gegevens over hem worden behandeld (art. 10), het recht op minimuminformatie (over zijn rechten) wanneer die gegevens bij hem worden verzameld (art. 11), het recht op voorafgaande informatie in geval van verstrekking van gegevens aan een derde (art. 12), het recht van inzage (art. 13 en 14), een recht van verzet (art. 15) en een recht op beroep bij de rechter (art. 22 tot 25).

Zeer omstreden door economische belangengroepen is het recht op verzet, neergelegd in artikel 15 : als er een «gewettigde» reden voor is, kan iedere betrokkene zich verzetten tegen behandeling van «zijn» gegevens (128).
Dat zal o.i. het geval zijn, wanneer de gegevens op heimelijke wijze worden ingezameld. Het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn kent geen mogelijkheden voor groepsactie door belangenorganisaties zoals dat bestaat in de Nederlandse Wet persoonsregistraties (129).

4. Personeelsprofielen

Een wat aparte plaats wordt ingenomen door artikel 16 dat geautomatiseerde individuele besluiten regelt. De betrokkene «heeft het recht *niet* te worden vermeld in een voor hem/haar bezwarend administratief of particulier besluit dat louter op grond van een persoonlijkheidsprofieloplevernde geautomatiseerde behandeling van gegevens is genomen». Dat betekent dat niemand het voorwerp kan zijn van een benadelende beslissing, welke een beoordeling van zijn gedrag inhoudt die uitsluitend gesteund is op een geautomatiseerde behandeling van persoonsgegevens.
Zo wordt het belang beschermd dat de betrokkene heeft bij een deelname aan de totstandkoming van voor hem belangrijke beslissingen. Het gebruik door machtige instellingen van door behandeling van gegevens verkregen profielen berooft de betrokkene van de mogelijkheid invloed uit te oefenen op het besluitvormingsproces, indien beslissingen op de enkele grondslag van zo'n profiel worden genomen. Handelt b.v. in strijd met de richtlijn, de werkgever die een werkzoekende afwijst, enkel en alleen op grond van de resultaten van een met behulp van de computer uitgevoerde psychotechnische beoordelingstest. Hetzelfde geldt wanneer via dergelijke beoordelingsapparatuur lijsten worden gemaakt waarop cijfers staan die de sollicitanten in volgorde van voorkeur rangschikken, enkel en alleen op grond van een persoonlijkheidstest (130).

De Lid-Staten moeten dus een bepaling opnemen die toelaat om elke beslissing m.b.t. zijn persoon te betwisten, als die uitsluitend gebaseerd is op een gedragsbeoordeling op grond van automatisch behandelde gegevens (131). In het gewijzigd voorstel werd dit verbod op geautomatiseerde beslissingen aanzienlijk verzacht in vergelijking met de eerste tekst : de Lid-Staten kunnen uitzonderingen toelaten in het kader van het sluiten of de uitvoering van een overeenkomst, mits aan het verzoek van de betrokkene is voldaan of passende maatregelen, waaronder de mogelijkheid zijn/haar standpunt te doen gelden, worden genomen ter bescherming van zijn/haar gerechtvaardigd belang. Dat kan ook indien de afwijking zijn grondslag vindt in een wet (art. 16 lid 2).

5. Besluit

De voorstellen van de Commissie garanderen een hoog privacybeschermingsniveau. M.b.t. controletechnieken onthouden we dat klank – en beeldgegevens uitdrukkelijk onder persoonsgegevens worden gebracht en dat het begrip behandeling niet gekoppeld wordt aan één bepaalde technologie. Spionage- en controletechnieken zijn bijgevolg onderworpen aan het systeem van het voorstel, en meteen aan de basisbeginselen inzake gegevensbehandeling. Verborgen apparatuur wordt uitgesloten krachtens het voorschrift dat de behandeling, en meteen de inzameling, «eerlijk en rechtmatig» behoren te zijn. De mogelijkheden om een «toestemming» tot behandeling af te dwingen, worden beperkt. E-mail wordt onder het toepassingsdomein van het voorstel begrepen en m.b.t. profielen is een specifieke verbodsbepaling opgenomen.

Wordt dit C.E.G.-gewijzigd Voorstel van Privacyrichtlijn zonder al te veel wijzigingen aangenomen, dan zal de Belgische wetgever wellicht verplicht zijn de Privacywet te herdenken en is de kans groot, dat het arbeidsrecht (eindelijk) een duidelijk antwoord op controle- en spionagetechnieken krijgt.

V. Slotbeschouwingen

In deze bijdrage ging de aandacht naar de algemene beginselen van gegevensbescherming, en in hoofdzaak naar het transparantieprincipe. Uit een correcte toepassing van dit principe vloeit een voorafgaande mededelingsplicht voort voor elke partij die controleapparatuur wil aanwenden. Een geheime toepassing van die technieken is onmogelijk. Het Verdrag van Straatsburg, de aanbevelingen van de Raad van Europa, de voorgestelde richtlijn van de E.G. en, zij het dan in mindere mate, de Belgische Privacywet laten hieromtrent geen twijfel bestaan.

Aan het nut van die procédés kan bovendien getwijfeld worden : een werkgever die het spel eerlijk speelt met zijn personeel, bereikt hoogstwaarschijnlijk eenzelfde efficiënt resultaat. Ook in de Verenigde Staten wordt gewerkt aan wetgeving, die de werkgever verplicht tot voorafgaande informatieverstrekking (132) : de voorgestelde *Privacy for Consumers and Workers Act* laat elektronische controle enkel toe voor het verzamelen van informatie nuttig voor het werk, en laat dit in voorkomend geval vergezeld gaan van flitslichten, hoorbare signalen of andere aanwijzingen die de werknemers ervan op de hoogte brengen dat hun activiteiten gevolgd worden.

De vraag naar de opportuniteit van controleapparatuur (m.a.w. naar het recht van werknemers op opaciteit (133)) kan pas aan bod komen als de idee van een mededelingsplicht ingang gevonden heeft, en zo de voorwaarden tot discussie en onderhandelingen vervuld worden. Belangrijk daarbij is de vraag naar het niveau waarop deze discussie moet gevoerd worden. Moeten nieuwe ontwikkelingen aan de rechtspraak en de sociale partners worden overgelaten, of moet de wetgever optreden ? Bij ontstentenis van specifieke wetgeving kan de rechtspraak o.i. te rade gaan bij het Verdrag van Straatsburg in samenlezing met het E.V.R.M.

Caspers ziet evenwel weinig heil in rechtsbescherming via de rechtspraak (134) : te vaak beperkt deze zich tot een belangenafweging tussen de belangen van werknemer en werkgever, wat dikwijls in het voordeel van deze laatste uitvalt.

Zo kan het bedrijfseconomisch belang bij personeelsinformatiesystemen makkelijk hard gemaakt worden, door te wijzen op de steeds veranderende marktpositie van het bedrijf en de noodzaak aan juiste informatie over het arbeidsgedrag. De werknemer daarentegen kan als gevolg van het ontbreken van duidelijke bepalingen niet op voorhand inschatten hoever hij moet meegaan bij de informatieverstrekking en hij weet niet welke vormen van electronic monitoring toegelaten zijn. Van werknemerszijde heeft men bijgevolg belang bij collectieve onderhandelingen of wetgeving (met telkens de keuze tussen dwingende wetgeving of modelcodes) (135).

Collectieve onderhandelingen vormen ogenschijnlijk een goede oplossing. Door elektronische volgsystemen staat niet alleen het individuele recht op privacy, maar ook het «collectief» privacyrecht van de werknemers op het spel (136). België en Frankrijk kennen reeds decennia lang wetgeving die verplicht tot collectief onderhandelen over de introductie en het gebruik van nieuwe technologie (137).

In het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn is er ruimte voorzien voor nationale en internationale gedragscodes (art. 28 en 29), maar tevens wordt daartoe een bepaalde procedure opgelegd («voorafgaand onderzoek door de nationale toezichthoudende autoriteit»).

De Belgische wet laat toe bij een in ministerraad overlegd besluit, na advies van de Privacycommissie, nade-

re regels uit te werken voor bepaalde sectoren (art. 44 Privacywet).

Of er met de Europese richtlijn nog wel behoefte zal zijn aan sectoriële zelfregulering kan betwijfeld worden.
De voorgenomen privacyrichtlijn is op sommige plaatsen zo gedetailleerd, dat kan gevreesd worden dat bijkomende codes alleen maar waarborgverflauwing beogen.
Ook op plaatsen waar het voorstel minder precies is, rijzen er problemen. Uitsluitende normering door medezeggingsorganen legt op hen een grote druk om naast algemene normen ook bedrijfsgebonden normen te aanvaarden, waardoor er te grote sectoriële verschillen (en dus rechtsongelijkheid) ontstaan (138).

Bovendien moet het collectief arbeidsrecht rekening houden met de individueel gegarandeerde grondrechten.

In de KOMA-video-camera-zaak wees de rechter erop dat geen enkel collectief akkoord voorbij kan gaan aan de individuele rechten. Eén van de karakteristieken van het recht op privacy is immers dat de meerderheid het niet aan de minderheid kan ontzeggen (139).

Een specifieke (individuele) toestemming is volgens Delarue (140) vereist, wanneer de aantasting de normale uitoefening van het patronaal gezag overstijgt.

Wanneer de aantasting ingrijpender is dan nodig voor de normale uitoefening van het patronaal gezag, zou een individuele toestemming vereist zijn, met het gevolg dat niet langer gewerkt kan worden met collectieve onderhandelingsprocedures.
Delarues oplossing is begrijpelijkerwijze vaag van aard.
We herinneren eraan dat het Europees voorstel stringentere bepalingen m.b.t. de toestemming bevat, zodat enige voorzichtigheid geboden is.
Problematisch bij de aanbeveling van Delarue is (zoals de auteur zelf aangeeft) dat in de arbeidswetgeving de patronale prerogatieven vrij algemeen geformuleerd zijn, en dat bijgevolg een zeer groot veld beslagen kan worden door collectieve onderhandelingen, dit mogelijkerwijs ten nadele van de individuele werknemer.

Caspers is dan ook een voorstander van door de wetgever te formuleren *minimum rights* inzake personeelsvolgsystemen :
1. de plicht van de werkgever om de werknemer te informeren over het gebruik van een personeelsvolgsysteem (*openess*);
2. toegang tot de dossiers (*individual participation*);
3. het verbod gegevens te verzamelen die niet relevant zijn voor de werkprestatie (*purpose specification* en *data quality*);
4. het verbod gegevens verkregen via «electronic monitoring» als uitsluitende basis te gebruiken voor werkevaluatie, tenzij de werknemer een recht van de werkgever heeft gekregen op een weerwoord binnen redelijke termijn (beperking van het gebruik van profielen);
5. het recht voor de werknemer na inzage van de verzamelde gegevens een eigen visie erop te geven (*dissenting opinion*);
6. juridische afdwingbaarheid van voornoemde principes.

Verwijzingen

(1) Privacywet : Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.*, 18 maart 1993.
(2) Rb. Luik, 11 maart 1987, *Dr. Inform.*, 1988/1, 45-46, met noot POULLET, Y.; *Computerr.*, 1988/2, 94-97; *D.C.C.R.*, 1988-89, 65-66, met noot POULLET, Y. Zie ook met BUYLE, J., LANOYE, L. en WILLEMS, A., «L'informatique. Chronique de jurisprudence (1976-1986)», *J.T.*, 1988, 93.
(3) Deze worden in het vonnis gedistilleerd uit de *in casu* niet toepasselijke wetgeving op de registratie van afbetalingsovereenkomsten waarin de «verbruikerskredietcentrale» van de Nationale Bank wordt genormeerd (*cf.* K.B. 15 april 1985 betreffende de registratie van afbetalingscontracten, *B.S.*, 20 april 1985). *Cf.* de noten van Yves Poullet bij dit vonnis (vorige voetnoot).
(4) Luik, 5 juni 1991, *J.T.*, 1992, 36-38, op p. 38 : «(...) le système (...) est constitutif de faute génératrice de responsabilité dans la mesure où il *méconnaît les droits essentiels de la personne privée* et porte gravement atteinte à la protection du consommateur de crédit».
(5) Vred. Namen, 13 januari 1987, *Computerr.*, 1988/2, 91-93, met noot POULLET, Y. en *Dr. Inform.*, 1987/3, 181-183, met noot POULLET, Y. Zie ook BUYLE, J., LANOYE, L. en WILLEMS, A., *o.c.*, 114.
(6) De vrederechter bedoelt het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van geautomatiseerde persoonsregistraties (17 juli 1985), *Gedr. St.*, 1984-85, 1330/1, 13 p.
(7) Art. 1 E.V.R.M. : «De hoge verdragsluitende partijen verzekeren eenieder, die ressorteert onder haar rechtsmacht, de rechten en vrijheden welke zijn vastgesteld in de eerste titel van dit verdrag». Zie o.a. GANSHOF VAN DER MEERSCH, W.J., «La garantie de droits de l'homme et la cour européenne de Strasbourg», *J.T.*, 1982, 105-106 en RIGAUX, F., *La vie privée. Une liberté parmi les autres* ?, Travaux de la faculté de droit de Namur/Larcier, Namur/Bruxelles, 1992, nr. 41, 38-39.
(8) Zie o.a. GANSHOF VAN DER MEERSCH, W.J., «L'ordre public et les droits de l'homme», *J.T.*, 1968, 663 en VELU, J., *Les effets directs des instruments internationaux en matière de droits de l'homme*, Brussel, Swinnen – Prolegomena, 1982, 30. Het Hof van Cassatie besliste in een opgemerkt en nagevolgd arrest dat de Belgische rechtsinstan-

ties de interne rechtsnormen, zelfs die van openbare orde, slechts kunnen toepassen, indien zij conform zijn aan de bepalingen van internationale verdragen die in België directe werking hebben. Cass., 27 mei 1971, *Pas.*, 1971, I, 886-920, met conclusie GANSHOF VAN DER MEERSCH. Zie ook VELU, J. en ERGEC, R., *La convention européenne des droits de l'homme*, Brussel, Bruylant, 1990, 84.

(9) Art. 8 E.V.R.M. stipuleert : «1. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling; 2. Geen inmenging van enig openbaar gezag is toegestaan m.b.t. de uitoefening van dit recht dan voor zover bij wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van rechten en vrijheden van anderen». Het art. 8 E.V.R.M. overschaduwt een aantal gelijkaardige bovennationale bepalingen, zoals art. 12 Universele Verklaring van de Rechten van de Mens en art. 17 Internationaal Verdrag inzake Burgerrechten en Politieke Rechten, alleszins wat de Europese rechtsorde betreft.

(10) VELU, J. en ERGEC, R., *o.c.*, 531-532. Dat betekent dat men zich op het artikel kan beroepen om schendingen van de privacy te doen stopzetten of er schadevergoeding voor te bekomen. Over de sancties bij schending van art. 8 E.V.R.M. in het Belgische recht, zie o.a. OVERSTEYNS, B., «Het recht op eerbiediging van het privé-leven», *R.W.*, 1988-89, 496-498.

(11) RIMANQUE, K. en PEETERS, P., «De toepasselijkheid van de grondrechten in de betrekkingen tussen private personen», in *De toepasselijkheid van de grondrechten in private verhoudingen*, RIMANQUE, K. (ed.), Antwerpen, Kluwer, 1982, 5.

(12) Op de controverse omtrent de zogenaamde *Drittwirkung*, derdenwerking of privaatrechtelijke werking van grondrechten wordt hier niet ingegaan. Enkel wordt vastgesteld dat het recht op eerbied van het privé-leven – en dus de vrijheid van dat laatste – geëerbiedigd moet worden zowel door de overheid als door particuliere maatschappelijke actoren. Tot dezelfde conclusie, zij het dan op andere gronden gesteund, komen talrijke auteurs, zoals o.a. DE MEYER, J., «Preadvies. Het recht op eerbiediging van het privé-leven, van de woning en van mededelingen in de betrekkingen tussen particulieren en de verplichtingen die daaruit voortvloeien voor de staten die partij zijn bij het verdrag», in *Privacy en rechten van de mens*, Leuven, Acco, 1974, 251-271; GANSHOF VAN DER MEERSCH, W.J., «Rede bij openingsvergadering», in *Privacy en rechten van de mens*, 6; HUMBLET, P., «Schipper naast God : enkele bedenkingen bij het bevelrecht van de werkgever», *Soc. Kron.*, 1991, 1, 5; RAUWS, W. en SCHYVENS, H., «De bescherming van werknemersgrondrechten binnen de individuele arbeidsverhouding», in *De toepasselijkheid van de grondrechten in private verhoudingen*, 180-183; RIGAUX, F., «Protection de la vie privée : questions d'actualité», *Ann. Dr.*, 1984/1-2 (themanummer : Protection de la vie privée), 6; RIGAUX, F., *La vie privée. Une liberté parmi les autres* ?, *l.c.*, nr. 48 en 134; RIMANQUE, K., «De gelding van de fundamentele rechten en vrijheden in de betrekkingen tussen privépersonen naar Belgisch recht, met enkele algemene besluiten», in *Privacy en rechten van de mens*, 283 (Rimanque noemt de negatie van de gelding van de fundamentele rechten en vrijheden in particuliere verhoudingen «een *contradictio in terminis, een anomalie*»); VAN GERVEN, W., «Principe de proportionnalité, abus de droit et droits fondamentaux», *J.T.*, 1992, 308 (de auteur verkiest echter de theorie van de indirecte werking); VELU, J., *o.c.*, 31-32; VELU, J. en ERGEC, R., *o.c.*, 74-78, 534-535 (met de aldaar aangehaalde rechtspraak en rechtsleer). Voor een historische duiding, zie KAYSER, P., *La protection de la vie privée*, Parijs/Marseille, Economica/Presses universitaires d'Aix-Marseille, 1990, 44-49.

(13) Zie RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Brussel/Parijs, Bruylant/L.G.D.J, 1990, 683-685.

(14) De aantasting zal evenwel ook mogelijk zijn op basis van een door het Europees Hof voor de Rechten van de Mens equivalent bevonden rechtsbron.

(15) *Cf.* RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Brussel/Parijs, Bruylant/L.G.D.J, 1990, 141-142. Over het proportionaliteitscriterium in het algemeen, zie VAN GERVEN, W., *o.c.*, 305-309; VAN GERVEN, W., «Beginselen van behoorlijk bestuur», *R.W.*, 1982-83, 975-976 en VAN GERVEN, W., *Hoe Blauw is het bloed van de prins* ?, Kluwer Rechtswetenschappen, 1983, i.h.b. op p. 16, 44-45. Voor de toepassing van het proportionaliteitsbeginsel op het vlak van de bescherming van persoonsgegevens, zie het mooie POULLET, Y. en LEONARD, Th., «Les libertés comme fondement de la protection des données nominatives», in RIGAUX, F., *La vie privée. Une liberté parmi les autres* ?, Travaux de la faculté de droit de Namur/Larcier, Namur/Bruxelles, 1992, 231-277.

(16) Zie RIGAUX, F., *o.c.*, 683-685.

(17) VAN DER HEIJDEN, P.F., *Grondrechten in de onderneming*, Deventer, Kluwer, 1988, 14.

(18) *Ibid.*

(19) Arbrb. Brussel, 26 maart 1990, *Soc. Kron.*, 1992, 154.

(20) Illustratief is ook dat Oversteyns – waarschijnlijk omdat zulks t.o.v. de rechters meer bruikbaar is – de problematiek van de privacy van de sollicitant, buiten een korte verwijzing naar art. 8 E.V.R.M., eveneens volledig in het teken plaatst van arbeids- en burgerrechtelijke middelen; OVERSTEYNS, B., «Recht op informatie van werkgever, recht op privacy van sollicitant. Enkele juridische problemen rond sollicitatie en aanwerving», *Or.*, 1988, 178-186.

(21) RAUWS, W. en SCHYVENS, H., *o.c.*, 222. Rauws en Schyvens stellen meer algemeen dat de contractvrijheid zich binnen de perken van de grondrechten moet doorzetten. Zulks negeren zou volgens hen betekenen dat de contractvrijheid als norm hoger zou ingeschat worden dan b.v. art. 8 E.V.R.M. Zij voegen daar evenwel onmiddellijk aan toe dat hun standpunt in ongelijke contractuele verhoudingen bijdraagt tot de *versterking* van de contractuele vrijheid of wilsautonomie van de zwakkere partij (180-181).

(22) HUMBLET, P., *De gezagsuitoefening door de werkgever. Een juridische analyse*, II, doctoraal proefschrift, Antwerpen, U.I.A., 1992, 428-429.

(23) O.E.S.O.-Richtlijnen : «O.E.C.D.-Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 september 1980» in *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, O.E.C.D., 1980, 9-12; *International Legal Materials*, 1981, I, 317.

(24) Verdrag van Straatsburg : «Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981» in *European Treaty Series*, nr. 108; International Legal Materials, 1981, I, 422; Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (vertaling), 28 januari 1981, *Gedr. St.*, Kamer, 1990-91, 1312/1, 32-41.

(25) C.E.G.-gewijzigd voorstel van privacyrichtlijn : COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, «Gewijzigd voorstel voor een richtlijn van de Raad betreffende de bescherming van natuurlijke personen i.v.m. de behandeling van persoonsgegevens en betreffende het vrije verkeer van die gegevens», COM (92) 422 def. – SYN 287, Brussel, 15 oktober 1992, 143 p.

(26) «Explanatory memorandum to the O.E.C.D.-Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data», in *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, O.E.C.D., 1980, 22-25. Zie ook DE HOUWER, J., «De bescherming van automatische persoonsgegevens en informaticacriminaliteit» in *Informaticacriminaliteit*, DE SCHUTTER, B. (ed.), Antwerpen, Kluwer, 1988, 587

(27) *Cf. Explanatory memorandum to the OECD-Guidelines*, 28-32; DE HOUWER, J., *o.c.*, 577-578; DE HOUWER, J. en VAN BRABANT, K., *Privacy and transborder data flows*, Brussel, Centrum voor internationaal strafrecht – V.U.B., Oktober 1989, 21; FOSCANEANU, L., «La protection des données à caractère personnel contre l'utilisation abusive de l'informatique», *Journal du droit international*, 1982, nr. 1, 72-73 en KIRSCH, W.J., «The protection of privacy and transborder flows of personal data : the work of the Council of Europe, the Organization for Economic Co-operation and development and the European Economic community», *Legal issues on European integration*, 1982/2, 31-32.

(28) Toelichtend verslag bij het Verdrag van Straatsburg, *l.c.*, 15.

(29) De ratificatie zou nu mogelijk zijn, maar moet nog geschieden. Vermelden we daarbij het door de ministers Wathelet en Eyskens op voorbarige wijze ingediende wetsontwerp houdende goedkeuring van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, opgemaakt te Straatsburg op 28 januari 1981 (24 oktober 1990), *Gedr. St.*, Kamer, 1990-91, 1312/1, 41 p. Het enige artikel van dit ontwerp luidde laconiek dat het bedoelde verdrag in België «volkomen uitwerking zal hebben», evenwel zonder bepaling van tijdstip om-

dat er toen nog geen wet was die dat mogelijk zou gemaakt hebben.

(30) Zo voorziet de Belgische Privacywet in de uitbreiding van het toepassingsdomein : zo valt het houden van bestanden met manuele gegevens onder het toepassingsgebied van de wet. Dit geldt echter niet voor bestanden die gegevens bevatten m.b.t. rechtspersonen. Ook worden bepaalde soorten gegevens uitgesloten.

(31) COUNCIL OF EUROPE – COUNCIL OF MINISTERS, *Recommendation* nr. R (89) 2 of the Committee of Ministers to Member States on the Protection of Data used for Employment Purposes. Adopted by the Committee of Ministers, on 18 January 1989, 5 p.

(32) BLANPAIN, R., «Aids en drugs-Richtlijnen voor ondernemingen», *R.W.*, 1988-1989, 144-145. Twee van die richtlijnen, nl. openheid en evenredigheid, kwamen ook bovendrijven op een Leuvense studiedag («Prof. Blanpain : De werknemer moet op de hoogte zijn», *De Morgen*, 21 augustus 1992, 2) over het probleem van alcohol-, drug- en aidstests in bedrijven : de werknemer heeft het recht te weten wat er met zijn urine- of bloedstaal gebeurt (openheid) en een veralgemeend onderzoek van alle werknemers in een bedrijf is uit den boze (proportionaliteit).

(33) «De werknemer kan slechts ... via de Wet persoonsregistraties toegang krijgen, maar heeft daar of de Registratiekamer of de arrondissementsrechtbank voor nodig. Zo'n actie lijkt niet bevorderlijk voor een goede verstandhouding tussen de werknemer en de werkgever»: CASPERS, R., «Informatiebehoefte van werkgevers en privacy van werknemers», *Sociaal recht*, 1992, 9, 242.

(34) Zie deel 1 van deze bijdrage.

(35) Art. 19 *et seq.* Wet 8 april 1965 tot instelling van de arbeidsreglementen; hierover DE GOLS, M., «Het arbeidsreglement», *Or.*, januari 1988, 29.

(36) ALBERTIJN, M., HANCKE, B. en WIJGAERTS, D., «Technology agreements and industrial relations in Belgium», *New Technology, Work and Employment*, spring 1990, 21; DE SCHRIJVER, L., «Nieuwe technologieën en sociale verhoudingen», *R.W.*, 1984-85, 2593-2616 en STROOBANT, M., «Nieuwe technologieën en arbeidsverhoudingen : kritische beschouwingen bij C.A.O. nr. 39», in *Technologie en Recht*, DE VROEDE, P. (ed.), Antwerpen, Kluwer rechtswetenschappen, 1987, 295-352.

(37) POULLET, Y., WARRANT, F., met medewerking van QUECK, R., «Nouveaux compléments au service téléphonique et protection des données : à la recherche d'un cadre conceptuel», *Dr. Inform.*, 1990, 2, 18-24.

(38) HUMBLET, P., *o.c.*, II, nr. 214, 428-429.

(39) *Cf.* POULLET, Y. en LEONARD, Th., *o.c.* en VAN GERVEN, W., *o.c.*

(40) Parijs, 9 november 1966, *D.*, 1967, 273; Lyon, 21 december 1967, *D.*, 1969, 25. Recent heeft ook het Franse Hof van Cassatie deze zienswijze gehuldigd; Cass. Fr., 20 november 1991, *Droit Social*, 1992, 31.

(41) WAQUET, P., «Un employeur peut-il filmer à leur insu des salariés ?», *Droit Social*, 1992, 31.

(42) Zie hierover COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Dix ans d'informatique et libertés*, Parijs, Economica, 1988, 214; TALLARD, M., «La négociation des nouvelles technologies : éléments pour une comparaison de la France et de la R.F.A.», *Droit Social*, 1987, 2, 125.

(43) LENOIR, C. en WALLON, B., «Informatique, travail et libertés», *Droit Social*, 1988, 230.

(44) Cass., 16 januari 1992, *Droit Pénal*, 1992, juli, 8, met kritische noot. Art. 187 C.P. kan ook niet ingeroepen worden tegen de werkgever die overgaat tot het doorzoeken van de door werknemers gebruikte computers.

(45) Art. 368 C.P. ingevoerd door de Wet 17 juli 1970 luidt «Sera puni (...) quiconque aura volontairement porté atteinte à l'intimité de la vie privée d'autrui : 1, En écoutant, en enregistrant ou transmettant au moyen d'un appareil quelconque des paroles prononcées dans un lieu privé par une personne, sans le consentement de celle-ci; 2, En fixant ou transmettant, au moyen d'un appareil quelconque, l'image d'une personne se trouvant dans un lieu privé, sans son consentement. Lorsque les actes énoncés au présent article auront été accomplis au cours d'une réunion au vu et au su de ses participants, le consentement de ceux-ci sera présumé.»

(46) LENOIR, C. en WALLON, B., *o.c.*, 230 met verw. naar rechtspraak.

(47) Cass. fr. (Crim.), 19 mei 1981, *D.*, 1981, 544; WAQUET, P., rapport bij Cass., 20 november 1991 opgenomen in *Droit Social*, 1992, 31 onder de titel «Un employeur peut-il filmer à leur insu des salariés ?».

(48) Parijs, 4 juli 1990, *Gazette du Palais*, 2-3 augustus 1991, 10, noot.

(49) Wet nr. 78-17 6 januari 1978 «relative à l'informatique, aux fichiers et aux libertés», *Journal officiel*, 7 januari 1978, *err.* 25 januari 1978.

(50) «Une recommandation n'a pas de valeur juridique contraignante. Elle vise seulement à conseiller un comportement, à donner une orientation, à définir une ligne de conduite sous réserve de l'appréciation des juridictions compétentes»; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 74. Zie tevens LENOIR, C. en WALLON, B., *o.c.*, 216.

(51) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *12e rapport d'activité 1991*, Paris, La documentation française, 321.

(52) KUHNMUNCH, O., «Personnes, entreprises et relations de travail, éléments de jurisprudence», *Droit Social*, 1988, 386.

(53) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 319.

(54) Voor een beoordeling van deze aanbeveling van 15 oktober 1985 «relative à la collecte et au traitement d'informations nominatives lors d'opérations de conseil en recrutement» : LENOIR, C. en WALLON, B., *o.c.*, 217.

(55) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 320. *Cf.* MOLE, A., «Informatique et libertés du travail : les nouveaux enjeux», *Droit Social*, 1990, 1, 61 met verw.

(56) Art. 25, MOLE, A., *o.c.*, 61 met verwijzing naar een zaak hangende voor het Hof van Beroep te Parijs. Deze aanwending van de Wet van 6 januari 1978 buiten het domein van de informatica wordt mogelijk gemaakt door art. 45, dat art. 25 toepasselijk maakt op «fichiers non automatisés».

(57) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 320.

(58) *Ibid.*, 320-321 en 485-486. Zie ook LENOIR, C. en WALLON, B., *o.c.*, 225-226; MOLE, A., *o.c.*, 62.

(59) Antwoord op een Parl Vr., 18 maart 1991 geciteerd in COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 533. De Minister van Justitie baseert zich in dit antwoord evenwel op arbeidsrechtelijke rechtspraak.

(60) *Droit de l'informatique en des télécoms*, 1991/4, 99. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 524.

(61) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 474. Zie ook POULLET, Y., WARRANT, F., met medewerking van QUECK, R., *o.c.*, 19; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 219.

(62) Cass. fr., 23 mei 1991, *Gazette du Palais*, 27-28 oktober 1991, 11; FRANCILLON, J., «Infractions relevant du droit de l'information et de la communication», *Rev. sc. crim.*, 1992, 1, 107-109.

(63) *Cf.* MOLE, A., *o.c.*, 62.

(64) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 325.

(65) MOLE, A., *o.c.*, 63 met verwijzingen naar de C.N.I.L.-verslagen.

(66) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 182-186. Zie tevens «Green light for video-surveillance», in *Transnational Data and Communication Report*, 1992, maart-april, 37.

(67) Het zal evenwel nog minstens 18 maanden duren, te rekenen van de datum van publikatie, vooraleer alle bepalingen van de Privacywet in werking zullen treden; zie de K.B.'s die samen met de Privacywet in het *B.S.*, werden gepubliceerd.

(68) Reeds voordien waren een aantal normen van kracht die een aantal van de *data protection principles* hadden geïmplementeerd : Wet 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *B.S.*, 21 april 1984; K.B. nr. 141 30 december 1982 tot oprichting van een databank betreffende de personeelsleden van de overheidssector, *B.S.*, 13 januari 1983; Wet 15 januari 1990 houdende de oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, *B.S.*, 22 februari 1990 (*err.* : *B.S.*, 2 juni 1990 en *B.S.*, 2 oktober 1990; gewijzigd door Wet 6 augustus 1990, *B.S.*, 2 oktober 1990); Wet 12 juni 1991 op het consumentenkrediet, *B.S.*, 9 juli 1991, (i.h.b. art. 68 tot 78) en Wet tot wijziging van de Wet betreffende de politie over het wegverkeer, gecoördineerd op 16 maart 1968 en van de Wet 21 juni 1985 betreffende de technische eisen waaraan elk voertuig voor vervoer te land, de onderdelen ervan, evenals het veiligheidstoebehoren moeten voldoen, *B.S.*, 8 november 1990 .

(69) M.v.T. bij het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (6 mei 1991), *Gedr. St.*, Kamer, 1990-91, 1610/1, 4.

(70) Een overzicht van de wet is te vinden in CENTRUM VOOR INTERNATIONAAL STRAFRECHT, «De Belgische privacy-wetgeving, een eerste analyse», *R.W.*, 1993, 1145.
(71) De analogie wordt expliciet vastgesteld in M.v.T. bij het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (6 mei 1991), *Gedr. St.*, Kamer, 1990-91, 1610/1, 30. Daarbij mag natuurlijk de bedenking gemaakt worden dat het voor de privacy te hopen valt dat de analogie met het milieustrafrecht niet uitgebreid wordt tot de efficiëntie van dat laatste...
(72) Die commissie functioneerde voorheen al onder gezag van o.a. de Rijksregisterwet en Wet op de Kruispuntdatabank.
(73) Inleiding van de Vice-Eerste Minister van Justitie en Economische Zaken, Verslag namens de Commissie voor de Justitie uitgebracht door mevr. Merckx-Van Goey, *Gedr. St.*, Kamer, B.Z. 1991-92, 413/12, 3 en 12. Zie ook inleidende nota van de Minister van Justitie, Verslag namens de Commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St.*, Senaat, B.Z. 1991-1992, 445-2, 119.
(74) Het genoemde systeem is sterk geïnspireerd door het mechanisme dat krachtens art. 17 Franse Privacywet in het leven werd geroepen. De C.N.I.L. kan aldaar – op basis van haar reglementaire bevoegdheid – *normes simplifiés* uitvaardigen voor de meest gangbare categorieën van gegevensverwerkingen die kennelijk geen schending inhouden van het privé-leven en de vrijheden. Voor verwerkingen die met deze *normes simplifiés* overeenstemmen, moet de houder – in plaats van een volledige aangifte in te dienen – alleen een verklaring van conformiteit met de normen neerleggen. De *normes simplifiés* worden door de C.N.I.L. opgesteld in overleg met de betrokken sectoren in functie van het bestaan van een reeks beperkende voorwaarden, die het kennelijk ongevaarlijke karakter van de verwerkingen moeten verzekeren : beperkte en nauwkeurig geformuleerde finaliteiten, «objectieve gegevens» die op eenvoudige wijze door de betrokkenen kunnen geraadpleegd worden, beperkte koppelingsmogelijkheden, enz. Tot zover werden reeds een 35-tal *normes simplifiés* uitgevaardigd die het grootste deel van de aangiften bestrijken (75-80 %). Zie hierover COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *o.c.*, 70-71 en VIVANT, M. en LE STANC, C., *Lamy droit de l'informatique*, Paris, Lamy S.A., 1986, 941 *et seq.* In het Belgisch systeem van vereenvoudigde aangiften of vrijstelling daarvan, is het niet de commissie maar de Koning, die de uiteindelijke beslissing neemt.
(75) DELARUE, R., «Bescherming van de privacy in de ondernering en de begrenzing van de patronale prerogatieven», *Soc. Kron.*, 1992, 4, 141.
(76) «Niet toegestaan evenwel is het geheel of gedeeltelijk afstaan van een personeelsbestand met het oog op de aanwending ervan naar aanleiding van sociale verkiezingen, zoals dat zich reeds heeft voorgedaan in Frankrijk», M.v.T. bij het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (6 mei 1991), *Gedr. St.*, Kamer, 1990-91, 1610/1, 10-11.
(77) Aan de opbouw en opvatting van de Privacywet ligt de idee ten grondslag dat de scheiding van machten een goede manier is om de ontsporing van macht te voorkomen; Herbert Burkert aangehaald in POULLET, Y. en LEONARD, Th., *o.c.*, 243. Zie ook POULLET, Y., «Informatique et libertés : un débat en quête de solution. Le projet de loi Wathelet», *Journal de reflexion sur l'informatique*, nr. 17, juli 1990, 30.
(78) Gegeven daarbij dat «elke» geautomatiseerde verwerking moet aangegeven worden (art. 17 § 5), impliceert zulks dat er voor elk doel van één verwerking sprake is, met dien verstande dat de verschillende verwerkingen gebruik kunnen maken van dezelfde gegevens. «Doel» mag hierbij echter wel in generieke termen begrepen worden. Het principe is wel degelijk : één generiek doel = één verwerking = één aangifte. Een verwerking dient alsdan beschouwd te worden als het geheel van bewerkingen strekkende tot de verwezenlijking van een *generieke finaliteit*, d.w.z. een geheel van verwante doelen – één soort doelen – die op redelijk onderscheidende manier onder één noemer kunnen gegroepeerd worden. *Cf.* advies van de Commissie voor de bescherming van de persoonlijke levenssfeer betreffende het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bijlage 1 bij het Verslag namens de Commissie voor de Justitie uitgebracht door mevr. Merckx-Van Goey, *Gedr. St.*, Kamer, B.Z. 1991-92, 413/12, 80.
(79) POULLET, Y. en LEONARD, Th., *o.c.*, 269-271 (met verwijzingen naar het hanteren van de proportionaliteitsregel door de *Commission nationale de l'informatique et des libertés*).
(80) Desgevallend kan op advies van de commissie van deze informatieplicht worden afgeweken of kan er voorzien worden in een procedure van collectieve kennisgeving (art. 9).
(81) DUMORTIER, J. en CLAES, P., «Privacybescherming en gegevensverwerking bij het personeelsbeleid», *Or.*, 1993/1, 9.
(82) Voegt men daaraan toe dat de Belgische geregistreerde (werknemer) in tegenstelling tot zijn Franse collega (art. 26 Franse Privacywet) niet beschikt over een recht om zich te verzetten tegen de opname in een verwerking, dan begrijpt men dat het werkend Belgisch rechtsubject een vrij passieve rol toebedeeld krijgt.
(83) Voor een ruime interpretatie van de contractuele verhouding wordt ook effectief gepleit : «De minister herinnert eraan dat beoogd werden de gevallen waarbij een persoon redelijkerwijze moet kunnen weten dat zijn verzoek om tussenkomst tot gevolg heeft dat zijn naam in een bestand wordt opgenomen. Het gaat dus inderdaad niet om een enge contractuele relatie», Verslag namens de Commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St.*, Senaat, B.Z. 1991-92, 445-2, 93.
(84) Opgenomen in HOLVAST, J., KETELAAR, R. en DE BAKKER, K., *Wet persoonsregistraties. Een praktische handreiking*, Amsterdam, Stichting Waakzaamheid Persoonsregistraties, 1990, 125 *et seq.*
(85) In de M.v.T. wordt zulks als volgt gerechtvaardigd : «Het ontwerp bepaalt niet hoe die informatie moet worden verstrekt teneinde de regeling zo soepel mogelijk te houden. De informatie kan schriftelijk of mondeling worden medegedeeld : het komt toe aan de verantwoordelijken voor het verzamelen van de gegevens om na te gaan of het noodzakelijk is dat zij het bewijs kunnen leveren dat voldaan is aan de hen opgelegde verplichtingen». Verder wordt daarbij echter gesteld dat het bezigen van formulieren «wel een bijzonder doeltreffende vorm van informatie zou zijn»: M.v.T. bij het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (6 mei 1991), *Gedr. St.*, Kamer, 1990-91, 1610/1, 9.
(86) *Cf.* het recht van verzet uit art. 26 Franse Privacywet. De vereiste van een voorafgaande kennisgeving zou enorme praktische problemen opwerpen (vertraging), aldus de Belgische minister : «De houder van het bestand zal ontzettend veel tijd verliezen indien hij pas met de registratie kan beginnen nadat alle betrokkenen verwittigd zijn»; Verslag namens de Commissie voor de Justitie uitgebracht door mevr. Merckx-Van Goey, *Gedr. St.*, Kamer, B.Z. 1991-92, 413/12, 44.
(87) *Ibid.*, 45. Dat is volgens hem de meest strenge en in de praktijk meest haalbare verplichting.
(88) M.v.T. bij het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (6 mei 1991), *Gedr. St.*, Kamer, 1990-91, 1610/1, 2 en inleiding van de Vice-Eerste Minister van Justitie en Economische Zaken, Verslag namens de Commissie voor de Justitie uitgebracht door mevr. Merckx-Van Goey, *Gedr. St.*, Kamer, B.Z. 1991-92, 413/12, 5 : «Het ontwerp betreft slechts één aspect van de bescherming van de persoonlijke levenssfeer : namelijk de gegevensverwerking. Nog andere facetten moeten worden behandeld. Zo bijvoorbeeld inzake het afluisteren».
(89) Hoorzitting met de leden van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Verslag namens de Commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St.*, Senaat, B.Z. 1991-92, 445-2, 15-16.
(90) *Ibid.*, 19.
(91) Het lid voegde daar verder aan toe dat zulks in elk geval de opvatting van de Franse C.N.I.L. is, die «op talrijke wijzen is tussengekomen o.m. voor conventionele foto's, waar men b.v. in grootwarenhuizen in Frankrijk de foto neemt van een chequeuitgever en de cheque. De C.N.I.L. heeft gezegd dat deze foto's moeten worden vernietigd als de cheque is geïnd zonder problemen. Zij is ook tussengekomen voor andere problemen zoals videoopnamen, waaraan zij ook beperkingen heeft opgelegd. De spreker denkt dat het volledig onder het concept van onze wet zou kunnen vallen. Dat is natuurlijk iets dat moet worden besproken»; *ibid.*, 19-20.
(92) Dumortier en Claes hebben zich in dit tijdschrift over deze vraag gebogen, en we bouwen voort op hun bevindingen, die overigens lijken te stroken met die van het laatstgenoemde lid van de commissie; zie DUMORTIER, J. en CLAES, P., *o.c.*, 3-13.
(93) Over de verhouding tussen gegevens en informatie : zie GUTWIRTH, S., *Waarheidsaanspraken in recht en wetenschap. Een onderzoek naar de verhouding tussen recht en wetenschap met bijzondere illustraties uit het informaticarecht*,

Brussel/Antwerpen-Apeldoorn, VUBPress/MAKLU, 1993 (ter perse), hfdst. 4, V.B.3.2.

(94) DUMORTIER, J. en CLAES, P., *o.c.*, 5.

(95) Het geheel van persoonsgegevens die in een louter alfabetische of chronologische volgorde worden bewaard, vormt geen «bestand». *Cf.* Verslag namens de Commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St.*, Senaat, B.Z. 1991-92, 445-2, 48. *Cf.* «Worden *a fortiori* van de werkingsfeer van deze wet uitgesloten : boeken en andere schriftelijke publikaties zoals telefoonboeken», M.v.T. bij het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (6 mei 1991), *Gedr. St.*, Kamer, 1990-91, 1610/1, 5.

(96) Dit is een *a contrario*-lezing van DUMORTIER, J. en SURMONT, J., «Het Belgische ontwerp over de bescherming van persoonsgegevens in Europees perspectief», *Computerr.*, 1992/1, 17.

(97) DUMORTIER, J. en CLAES, P., *o.c.*, 7. Ook onderzoeken zij de vraag of aan werknemers nu een recht van inzage moet verleend worden in personeelsdossiers, schriftjes en kladboeken.

(98) Robben laat daarover geen twijfel bestaan : «Op geautomatiseerde wijze betekent echter niet zondermeer computerondersteund, maar doelt op alle technieken waarbij één of meerdere bewerkingen niet rechtstreeks door de menselijke hand worden gestuurd»; ROBBEN, F., «Het wetsontwerp Wathelet tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens», *Computerr.*, 1992/1, 3.

(99) *Cf.* DUMORTIER, J. en CLAES, P., *l.c.*, 7.

(100) In het geval dat de controletechniek dient beschouwd te worden als een manueel bestand, zal de commissie logischerwijze de aangifte moeten eisen, omdat het gebruik van zo'n technieken sowieso «een mogelijke schending van de persoonlijke levenssfeer inhoudt».

(101) Advies van de Raad van State, Wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (6 mei 1991), *Gedr. St.*, Kamer, 1990-91, 1610/1, 53-54 en Advies nr. 10/92 van 20 augustus 1992 van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, bijlage II bij Verslag namens de Commissie voor de Justitie, uitgebracht door de heer Vandenberghe, *Gedr. St.*, Senaat, B.Z. 1991-92, 445-2, 125.

(102) Hoorzitting met de leden van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Verslag namens de Commissie voor de Justitie, uitgebracht door de heer Vandenberghe, *Gedr. St.*, Senaat, B.Z. 1991-92, 445-2, 29.

(103) *Ibid.*, 28.

(104) Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer betreffende het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bijlage I bij het Verslag namens de Commissie voor de Justitie, uitgebracht door mevr. Merckx-Van Goey, *Gedr. St.*, Kamer, B.Z. 1991-92, 413/12, 84-85 en Advies nr. 10/92 van 20 augustus 1992 van de Commissie voor de bescherming van de persoonlijke levenssfeer, bijlage II bij Verslag namens de Commissie voor de Justitie, uitgebracht door de heer Vandenberghe, *Gedr. St.*, Senaat, B.Z. 1991-92, 445-2, 123-124.

(105) Zie ook DELARUE, R., *o.c.*, 125.

(106) I.A.O. nr. 11, Goedkeuringswet 6 mei 1977, *B.S.*, 23 september 1977.

(107) C.A.O. nr. 29 gesloten in de N.A.R. op 13 december 1983 betreffende de voorlichting en het overleg inzake de sociale gevolgen van de invoering van nieuwe technologieën. Algemeen verbindend verklaard bij K.B. 25 januari 1984, *B.S.*, 8 februari 1984.

(108) C.A.O. nr. 9 gesloten in de N.A.R. op 9 maart 1972 houdende ordening van de in de Nationale Arbeidsraad gesloten nationale akkoorden en collectieve arbeidsovereenkomsten betreffende de ondernemingsraden. Algemeen verbindend verklaard bij K.B. van 12 september 1972, *B.S.*, 25 november 1972.

(109) ALBERTIJN, M., HANCKE, B. en WIJGAERTS, D., *o.c.*, 28. De C.A.O. viseert immers in hoofdorde de produktieve aspecten van automatisatie en minder de controletoepassing ervan.

(110) KABEL, J.J.C., «Toezicht en controle op personeelsregistratie en de Wet persoonsregistraties», in *Privacy op de werkplek*, VAN DER HEIJDEN, P.F. (red.), Den Haag, S.D.U. juridische en fiscale uitgeverij, 1992, 83.

(111) Dat is noodzakelijk omdat de Lid-Staten met een reeds bestaand hoog beschermingsniveau begrijpelijkerwijs de maat van de harmonisatie stellen : moeilijk kan verwacht worden dat zij hun beschermingsniveau zouden verlagen.

(112) Eerste versie Voorstel van de Commissie van de Europese Gemeenschappen voor een richtlijn van de Raad betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens, COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *Mededeling van de Commissie betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens in de Gemeenschap en betreffende de beveiliging van informatiesystemen*, COM (90) 314 def. – SYN 287, Brussel, 24 september 1990 (Engelse versie : 13 september 1990), 31-56 en in *Computerr.*, 1990/5, 265-269.

(113) Als alternatief voor de preventieve procedurele benadering van de Europese Commissie werd uiteraard gepleit voor vrijwillige gedragscodes. Zie b.v. BELGISCHE VERENIGING VAN BANKEN, «Een voorstel voor een richtlijn inzake databestanden», *Europese informatie*, 14 november 1990, 4; BERKVENS, J.M.A., «COM (90) 314 Final – Syn 287 en 288, Brussel 13 september 1990», *Computerr.*, 1990/5, 263; BERKVENS, J.M.A., «Architecture of EC Data Protection», *Transnational data and communications report*, March-April 1991, 39; KROGER, H., «European Employers Federation Position on the Directive», *Transnational data and communications report*, March/April 1991, 46; UNICE, «UNICE Position on a Proposal for a council directive», *Transnational data and communications report*, March/April 1991, 47-50; X., «Business and EC debate data protection directives», *Transnational data and communications report*, January/February 1991, 28-29.

(114) *Minutes of the third meeting of the EC Data protection commissionners, Manchester*, 30 april 1991, 5. Zie ook DE SCHUTTER, B., «De weerslag van de nieuwe informatietechnologieën op de internationalisatie van de rechtsontwikkeling» in *Liber Amicorum Henri Vander Eycken*, Brussel, VUBPRESS, 1991, 286 en POULLET, Y., «Privacy protection and transborder data flow; recent legal issues» in *Advanced topics of law and information technology*, VANDENBERGHE, G.P.V. (ed.), Deventer, Kluwer, 1989, Computer/law series, nr. 3, 36-37.

(115) Zie M.v.T. bij het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn, 13.

(116) M.v.T. bij het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn, 10.

(117) Merken we op dat Berkvens en Schauss zich wat dat betreft vooral zorgen maken over de activiteiten van postzegelverzamelaars, terwijl zij zeer discreet blijven over visuele spionagetechnieken...; BERKVENS, J. en SCHAUSS, M., «De privacy-voorstellen van de Europese Commissie», *Computerr.*, 1992/3, 118 en BERKVENS, J. en SCHAUSS, M., «Tweede akte van de privacyrichtlijn», *Computerr.*, 1992/6, 238 (voetnoot 13).

(118) Art. 2b C.E.G.-gewijzigd Voorstel van Privacyrichtlijn : «Behandeling van persoonsgegevens : hierna 'behandeling' te noemen, elke verrichting of elk geheel van verrichtingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, uitwerken, wijzigen, opvraagbaar maken, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, verwijderen of vernietigen van gegevens».

(119) M.v.T. bij het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn, 10.

(120) I.v.m. de rechtmatigheid en eerlijkheid van de behandeling (*cf. infra*) stelt de Memorie uitdrukkelijk dat de bepaling doelt op de «behandeling» en dus «uiteraard het verzamelen van gegevens omvat»; *ibid.*, 15.

(121) *Ibid.*, 3.

(122) BERKVENS, J. en SCHAUSS, M., «Tweede akte», *o.c.*, 232.

(123) M.v.T. bij het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn, 15.

(124) In de gevallen van art. 7 onder b, c, e, en f, moet de betrokkene evenwel uiterlijk bij de eerste *verstrekking van gegevens aan derden* daarover in kennis gesteld worden en informatie verkrijgen; art. 12 C.E.G.-gewijzigd Voorstel van Privacyrichtlijn.

(125) BERKVENS, J. en SCHAUSS, M., «Tweede akte», *o.c.*, 233.

(126) M.v.T. bij het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn, 12. De intrekking heeft geen terugwerkende kracht, want dat zou een behandeling van persoonsgegevens die in eerste instantie rechtmatig was, met terugwerkende kracht onrechtmatig maken.

(127) Deze moet overeenkomstig het voorstel (en i.t.t. de Belgische Privacywet) voor categorieën van behandelingen die bijzondere risico's meebrengen, een voorafgaand onderzoek voeren; art. 18 4 C.E.G.-gewijzigd Voorstel van Privacyrichtlijn.

(128) Met geldige gronden wordt in deze bepaling bedoeld het ontbreken van een wettige grondslag voor een bepaalde behandeling van persoonsgegevens, bijvoorbeeld het feit dat met betrekking tot een bepaalde behandeling niet aan

rechtmatigheidsvereisten is voldaan; M.v.T. bij het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn, 26.
(129) OFFREINS, R., KETELAAR, R. en HOLVAST, J., «Gevolgen voor de Wet persoonsregistraties», *Privacy en Registratie*, 1992, 3, 18.
(130) M.v.T. bij het C.E.G.-gewijzigd Voorstel van Privacyrichtlijn, 27.
(131) *Ibid.*
(132) KRAY, J. en ROBERTSON, P., «Enhanced Monitoring of White Collar Employees : Should Employers Be Required to Disclose ?», *Univ. of Puget Sound Law Review*, 1991, herfstnummer, 166-170.
(133) Namelijk het recht niet blootgesteld te worden aan informatiegaring; LENOIR, C. en WALLON, B., *o.c.*, 214.
(134) CASPERS, R., *o.c.*, 241.
(135) Caspers haalt verschillende bezwaren aan tegen sectoriële modelcodes (o.a. precies het gegeven dat ze niet dekkend zijn voor alle sectoren van het bedrijfsleven); CASPERS, R., *o.c.*, 243.
(136) *Cf.* DE VRIES, H., «Studiemiddag Privacy op de werkplek», *Computerr.*, 1992/2, 80.
(137) TALLARD, M., *o.c.*, 124-129.
(138) CASPERS, R., *o.c.*, 244.
(139) Rb. Roermond, 12 september 1985, *Computerr.*, 1985, 54.
(140) DELARUE, R., *o.c.*, 135-136.